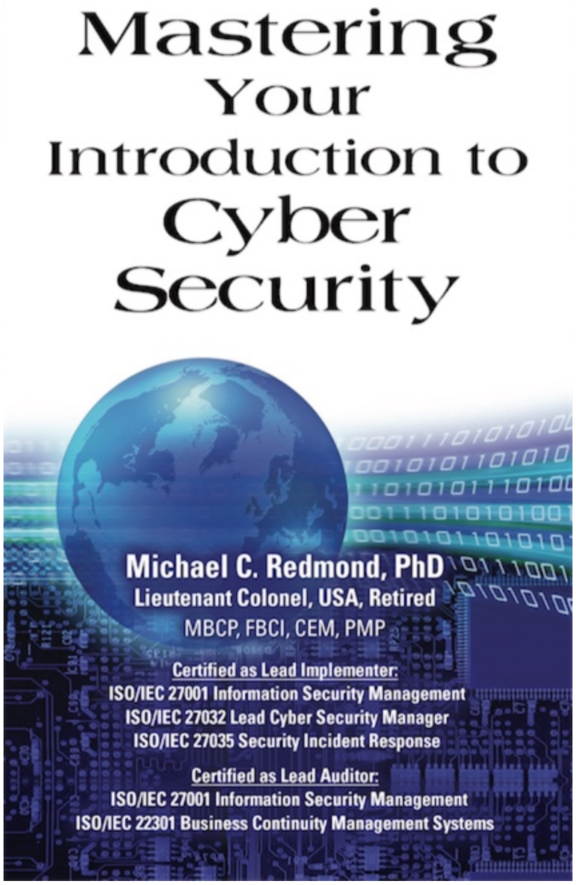


Mastering Your Introduction to Cyber Security

Michael C. Redmond, PhD
Lieutenant Colonel, USA, Retired
MBCP, FBCI, CEM, PMP

Certified as Lead Implementer:
ISO/IEC 27001 Information Security Management
ISO/IEC 27032 Lead Cyber Security Manager
ISO/IEC 27035 Security Incident Response

Certified as Lead Auditor:
ISO/IEC 27001 Information Security Management
ISO/IEC 22301 Business Continuity Management Systems

Cyber-attacks have increased exponentially, making this book essential in areas such as Business Management, Business Continuity and Disaster Recovery, Risk Management, Compliance, and IT. Dr. Michael C. Redmond, PhD takes a complicated subject and breaks it down into plain English...

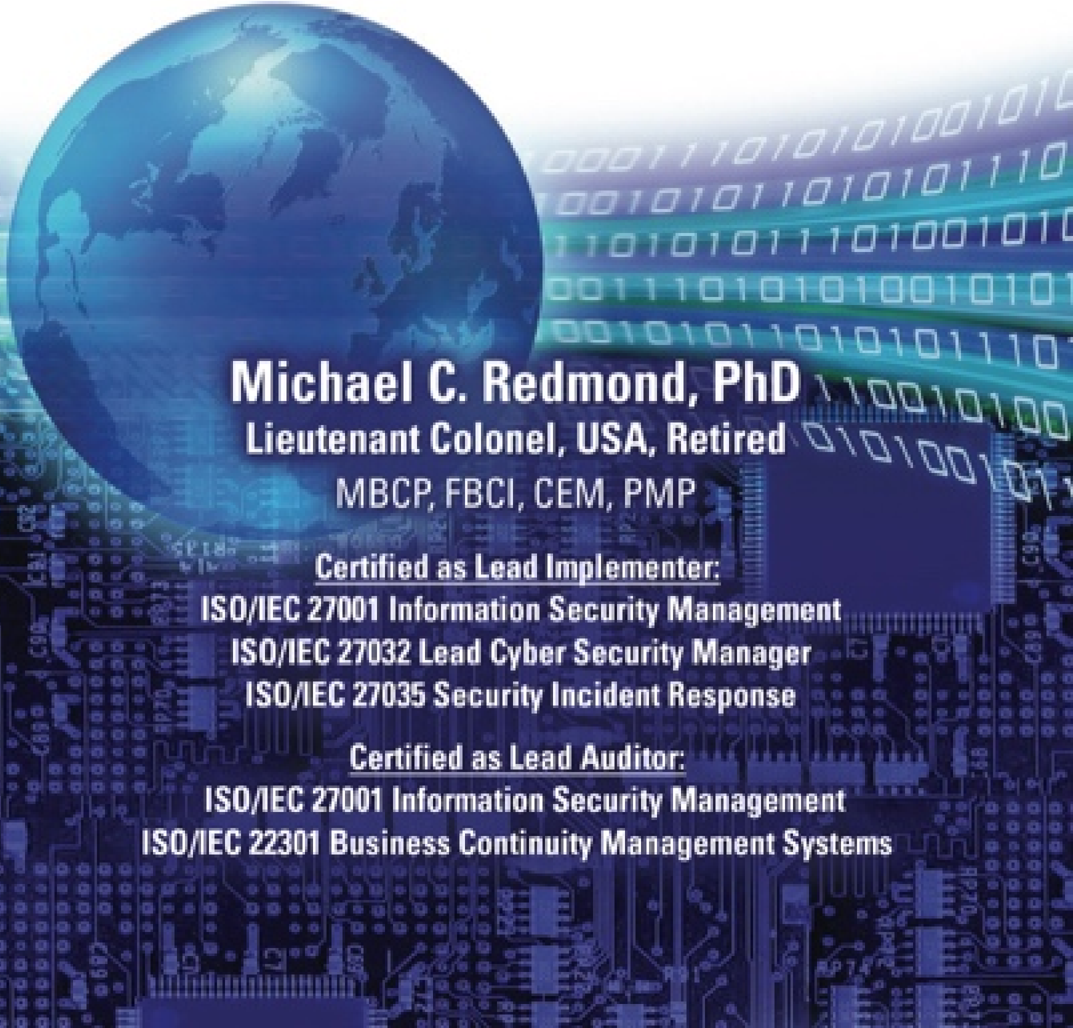
Mastering Your Introduction to Cyber Security

by Dr. Michael C. Redmond PHD

Order the complete book from the publisher
Booklocker.com

https://www.booklocker.com/p/books/9916.html?s=pdf
or from your favorite neighborhood
or online bookstore.

Mastering Your Introduction to Cyber Security



Michael C. Redmond, PhD

Lieutenant Colonel, USA, Retired

MBCP, FBCI, CEM, PMP

Certified as Lead Implementer:

ISO/IEC 27001 Information Security Management

ISO/IEC 27032 Lead Cyber Security Manager

ISO/IEC 27035 Security Incident Response

Certified as Lead Auditor:

ISO/IEC 27001 Information Security Management

ISO/IEC 22301 Business Continuity Management Systems

Hardcover ISBN: 978-1-63491-543-4
Paperback ISBN: 978-1-63491-418-5

Published by BookLocker.com, Inc., Bradenton, Florida.

Printed on acid-free paper.

BookLocker.com, Inc.
2018

First Edition

BookLocker

DISCLAIMER

This book details the author's personal experiences with and opinions about an introduction to cyber security.

The author and publisher are providing this book and its contents on an “as is” basis and make no representations or warranties of any kind with respect to this book or its contents. The author and publisher disclaim all such representations and warranties, including for example warranties of merchantability and information security and cyber advice for a particular purpose. In addition, the author and publisher do not represent or warrant that the information accessible via this book is accurate, complete or current.

The statements made about products and services have not been evaluated by the U.S. government. Please consult with your own legal or accounting professional regarding the suggestions and recommendations made in this book.

Except as specifically stated in this book, neither the author or publisher, nor any authors, contributors, or other representatives will be liable for damages arising out of or in connection with the use of this book. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory; direct, indirect or consequential damages; loss of data, income or profit; loss of or damage to property and claims of third parties.

You understand that this book is not intended as a substitute for consultation with a licensed medical, legal or accounting professional. Before you begin any change of your lifestyle in any way, consult a licensed professional to ensure that you are doing what’s best for your situation.

This book provides content related to Cyber Security and information security topics. As such, use of this book implies your acceptance of this disclaimer.

Table of Contents

Dr. Michael C. Redmond, PhD

About the Author

Dr. Michael C. Redmond, PhD is CEO of Redmond Worldwide, an International Consulting Company and consults, trains and audits in the areas of Cyber Program Management including Cyber Security Incident Response, Cyber Programs development, and training, SIEM – Security Information and Event Management. In addition, the company also consults in Business Continuity, Disaster Recovery, and Crisis Management.

The company can be accessed for more Information at www.redmondworldwide.com. Prior consulting experience includes both consulting and compliance auditing with such firms as Chubb, Deloitte and KPMG. She served four years on Active Duty with the U.S. Military and completed an additional 16 years with the National Guard and Reserve.

She is a Consultant, Trainer, Speaker, and Author. Michael also conducts ISO Certification Training for PECB. Michael an active member of Information Systems Security Association

(ISSA), ISACA, Project management Institute (PMI), Association of Contingency Planners and Contingency Planning Exchange. She has consulted and audited in the area of Cyber Security for clients internationally in the arenas of Healthcare, Insurance, Finance, and Manufacturing. Her projects have included:

- ❖ Compliance, Risk and Governance
- ❖ Developing full Cyber and Information Security Programs and Implementation
- ❖ SIEM Security Information and Event Management
- ❖ (CSIRT) Cyber Security Incident Response Programs, Plans, Playbooks, Training and Testing
- ❖ Table Top Tests
- ❖ Testing and Exercises
- ❖ Audit of Programs and Documentation
- ❖ Preparing Organizations for Certification
- ❖ Certification Audits
- ❖ Audit of CSIRT Programs and Documentation
- ❖ SIEM Security Information and Event Management - Combining software products and services combining security information management (SIM) and security event management (SEM)
- ❖ ISO Certification Trainer
- ❖ ISO Implementer Certification Training
- ❖ ISO Audit Certification Training
- ❖ Audit of CSIRT programs and documentation

She has been honored as a Top Woman in her field at a White House Luncheon and was selected out of the world to write the prologue for the chapter on RISK Management by the United Nations for their Disaster Book, which was given to the head of state for every UN member nation. Women of Distinction

Magazine named her on the list of “Women of Distinction for 2017” for her work in Cyber Security.

She served for a short time as the US Attaché to Chile for Disaster Recovery at the request of the President of Chile.

She is a Certified Business Recovery Planner; Certified Emergency Manager; and holds two Master Level Certifications in Business Continuity. She has ISO Certifications as Lead Implementer and Auditor.

Certified as Lead Implementer:

ISO/IEC 27001 Information Security Management
ISO/IEC 27032 Lead Cyber Security Manager
ISO/IEC 27035 Security Incident Response
ISO/IEC 22301 Business Continuity Management Systems
ISO/IEC 21500 Lead Project Manager
ISO 31000 Risk Management
ISO 55001 Asset Management
ISO/IEC 14001 Environmental Management
ISO 9001 Quality Management
ISO 26000 Social Responsibility
ISO 37001 Anti Bribery Management Systems

Certified Implementer – Foundation

ISO 22316 Resiliency Management
ISO 22320 Emergency Management
ISO 20700 Management Consultancy Services

Certified as Lead Auditor:

ISO/IEC 27001 Information Security Management
ISO/IEC 22301 Business Continuity Management Systems
ISO 55001 Asset Management
ISO/IEC 14001 Environmental Management
ISO 9001 Quality Management
ISO 26000 Social Responsibility

Other Certifications:

Masters Business Continuity Planning (Disaster Recovery Institute) - MBCP
Masters Business Continuity Planning (Business Continuity Institute) - FBCI
Certified Emergency Manager - CEM
Certified Project Manager – PMP
Certified Trainer PECB

She is also a graduate of Command & General Staff College out of Fort Leavenworth, where she studied strategic planning, control and command, and control in an emergency. Furthermore, she has completed Civil Affairs Advanced courses in the School for Special Warfare, which encompasses planning in various political and cultural environments.

She was an Adjunct Professor for Emergency Management and Business Continuity Management at New York University and the Masters program at John Jay College.

Dr. Redmond is an author and an International Speaker. She has written for many Contingency, Risk and Security magazines and has Audio Training Programs on Cyber Security and Business Continuity/Disaster Recovery and Emergency Management COOP and COG. Michael's Audio Trainings receive Continuing Education Units/Points (CEU) and (CEP) from Disaster Recovery Institute (DRI) and other certifying organizations.

- Cyber Security Training - 6 CEU's/CEP's
- Business Continuity Management - 20 CEU's/CEP's

www.rwknowledge.com

Chapter 3: Risks and Mitigations

About this Chapter

Cyber Security has its own inherent risks that can be mitigated, if not prevented. Understanding these risks and mitigations helps an organization strategize better.

Why Have Cyber Security?

The world today relies greatly on computing systems and the Internet for communication (email, mobile phones), entertainment (digital cable, mp3s), transportation (car engine systems, airplane navigation), shopping (online stores, credit cards), medicine (equipment, medical records), and it doesn't end here as technology grows to tailor our daily lifestyle choices. How much of our daily lives rely on computers? How much of our personal information is stored either on company owned systems, embedded applications, or within someone else's system?

Cyber security involves protecting that information by detecting, preventing and responding to attacks. It is a development of processes and best practices designed to protect networks, computers, programs and data damage or unauthorized access.

What Are The Risks?

There are many risks, some more severe than others. These dangers range from viruses erasing an entire system to someone breaking into the systems. Attackers are known for altering files, using the computer to attack others, stealing identities, and using others credit card and financial information to make unauthorized purchases. Attackers can open up other fake accounts and businesses utilizing this information in order to maximize gain. Even with the best protections, some of these things can happen to any organization or person. This is why it is important to establish best practice solutions. These solutions should be a part of the secure environment in order to minimize risk.

Security Policy

Human error causes most problems. Raising security awareness within the organization can help with mitigation. Government and organizational laptops are being lost, with sensitive data often finding its way into the public domain.

People often move corporate data around, perhaps sending it home for out-of-hours work, or forwarding it to a friend because there was something funny in it.
This is done without malice, but in ways that expose an organization to potential security and legal risk.

Better education for users would help eradicate these threats. Staff must be aware of their responsibilities regarding company and customer data, and there must be enforcement and adherence to policies.

Allow employees to have only approved software on their laptops and computer. Instruct employees to lockdown computers at the end of the night. Computers should be set up to allow lockdown by control/alt/delete or other such conformity.

Employee policies should prohibit access to unauthorized websites. In addition, the policy should prohibit opening, and especially passing along, emails that contain moving graphics. Employee abuse of email, instant messaging, and surfing for porn, eBay, sports and news sites is costing organizations lost productivity every year, but more importantly, it opens the organization to cyber terrorism. When employees know close monitoring exists, they drastically reduce the activities that harm your business. Consider a monitoring tool to reduce the risk and to enforce the security policy.

Cyber Terrorism or Cyber Attack?

“Attacker”, “intruder”, and “hacker” are terms applied to people who seek to exploit weaknesses in software and computer systems for their own gain. Although their intentions are sometimes fairly benign and motivated solely by curiosity, their actions are typically in violation of the intended use of the systems they are exploiting. The results vary from altering data, stealing, to no impact.

The FBI defines terrorism as the unlawful use of force or violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. Cyber attacks can be for political, financial, espionage and other reasons.

Both cyber-terrorism and cyber attacks can result in the use of using resources to intimidate or coerce others. An example of cyber-terrorism could be hacking into a hospital computer system to change someone's medicine prescription to a lethal dosage as an act of revenge. These things can and do happen.

Cyber attacks are becoming a viable option to traditional physical acts of violence due to:

- Anonymity
- Diverse targets
- Ease of operation from nearly any location
- Fewer resources are needed
- Low risk of detection
- Low risk of personal injury
- Low investment

Getting Started

List the main information that the organization does not want anyone to have. The areas under Cyber Security are broken down into hardware, software, network, automation, the users and the suppliers. Deal with the human side of Cyber Security in procedures. If you are doing business with a country that does not even have Cyber Security laws, then the risk is even higher. Malicious attacks are plentiful today.

Unfortunately, some individuals exploit the Internet through criminal behavior and other harmful acts. Criminals can try to gain unauthorized access to users' computers and then use that access to steal identities, commit fraud, or even launch cyber attacks against your organization. By following Cyber Security practices, users can mitigate the harm cyber criminals can cause. In adapting a security program, remember every PC is a possible area for attack.

Only the organization can determine what is actually at risk. If a thief steals a laptop, the most obvious loss is the machine itself. However, if the thief is able to access the information on the computer , all of the information stored on the device is at risk, as well as any additional accessed information of the data stored on the device itself.

Unauthorized people should not be able to access sensitive corporate information or customer account information. Even if there is not any sensitive corporate information on a laptop, think of the other information at risk: information about appointments, passwords, email addresses and other contact information, personal information for organization accounts, etc.

Awareness sessions for users are a good way to start. Cover such topics as

- Choosing and Protecting Passwords
- Understanding Anti-Virus Software
- Understanding Firewalls
- Coordination Virus and Spyware Defense
- Protect the organizations laptops
- Password-protect all computers. Make sure that users have to enter a password to log in to the computer
- Users should keep the laptop with them at all times. When traveling, users should keep their laptop with them at all times unless required by the airline to check the laptop. Meal times are optimum times for thieves to check hotel rooms for unattended laptops. If users are attending a conference or trade show, they must be especially wary. These venues offer thieves a wider selection of devices that are likely to contain sensitive information, and the conference sessions offer more opportunities for thieves to access guest rooms.
- Downplay laptops. There is no need for users to advertise to thieves that they have a laptop. When

possible, consider non-traditional bags for carrying laptops.

- Back up files. Someone else may be able to access information from a stolen device. To avoid losing all of the information, users should make incremental backups of important information and store the backups in a separate location until they can back up the information on the organizations system. Not only will they still be able to access the information, but also they will be able to identify and report exactly what information is at risk.
- Laptop Users Guidelines while on the road if unable to backup to the organization's backup system
    - Make sure users do a fire drill to make sure your backup system is working. It is astonishing how many users, when it comes time to restore, discover their backup are empty or are missing crucial data.
    - Keep offsite backups. If a user's computer in their office is damaged by fire, flood or theft, chances are, their individual onsite backups wi

Physical Security Is an Important Part of Cyber Security

Today's headlines include Data Breach, Denial of Service and so much more. Cyber Security and Risk Management is not only about preventing external attacks, but also identifying and protecting against the insider threat.

Passwords

One of the best ways to protect information or physical property is to ensure that only authorized people have access to it. Verifying that someone is the person they claim to be is the next step, and this authentication process is even more important, and more difficult, in the cyber world. Passwords are the most common means of authentication, but if users do not choose good passwords or keep them confidential, they are almost as ineffective as not having any password at all. Many systems and services have been successfully broken into due to the use of insecure and inadequate passwords, and some viruses and worms have exploited systems by guessing weak passwords.

Anti-Virus Software

Antivirus Software is an essential security application. Most antivirus products can remove detected malicious code and repair most damage caused by such malicious code. It’s one example of a host IDS. It monitors the local system for evidence of malware in memory, in active processes, and in storage.

In order for antivirus software to be effective, it must be kept current with daily signature-database updates. It is also important to use the most recent engine, because new methods of detection and removal are found only in the most current versions of antivirus software.

Once an organization installs an anti-virus package, users should scan their entire computer periodically.

- ❖ Automatic scans - Depending on what software the organization chooses, they may be able to configure it to automatically scan specific files or directories and prompt at set intervals to perform complete scans.

- ❖ Manual scans - It is also a good idea to have users manually scan files received from an outside source before opening them. This includes
  - o saving and scanning email attachments or web downloads rather than selecting the option to open them directly from the source
  - o scanning media, including CDs and DVDs, for viruses before opening any of the files

Firewalls

A firewall is a hardware or software component designed to protect one network from another. Firewalls provide protection by controlling traffic entering and leaving a network. Firewalls are typically deployed between areas of high and low trust zones, like a private network communicating to the public internet or between two networks that belong to the same organization, but are from different departments.

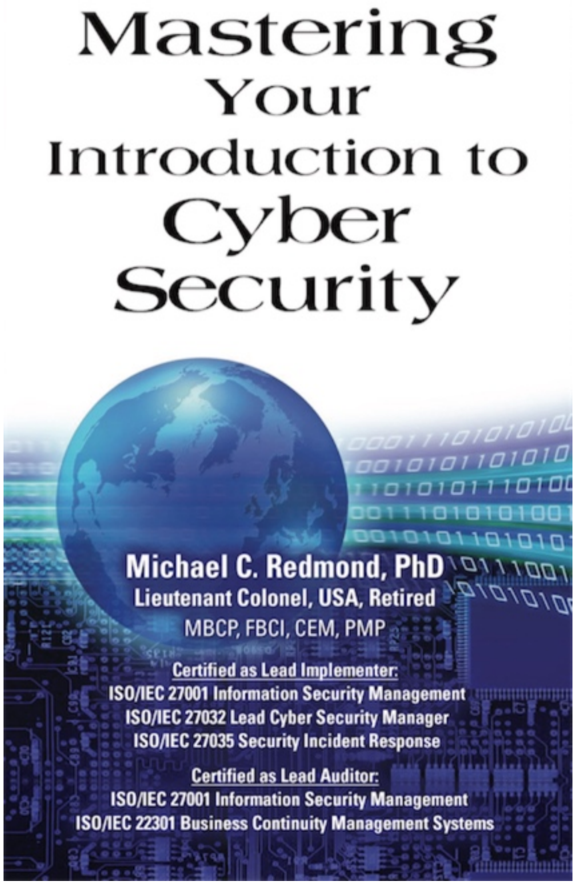
Spyware and Viruses

Spyware and viruses can interfere with an organization's ability to process information or can modify or destroy data. Some organizations believe that the more anti-virus and anti-spyware programs they install on the network and individual remote computers, the safer they will be. It is true that not all programs are equally effective, and they will not all detect the same malicious code. However, it is possible to introduce problems by installing multiple programs in an attempt to catch everything.

Malicious Code

Malicious code is a set of instructions designed to compromise the system, mobile device, laptop, desktop, server and other electronic systems that can run code. This category includes code such as viruses, worms, and Trojan horses. Although some people use these terms interchangeably, they have unique characteristics.

- Viruses – Any malicious software that is designed to affect system storage files, memory and running processes.
- Worms – Similar to a virus except that it propagates the virus so that it can spread across the network
- Trojan horses – Malicious software that hides itself as legitimate software. It masquerades as actual software, but it actually has remote controlled software underneath.
- Rootkits – Rootkits are ring 0 (Kernel Mode) / ring 3 (User Mode) that operate at the highest privilege level of the system designed to subvert the Operating System in an attempt to remain hidden from detection from the kernel.
- Exploit Kits – Exploit kits are obfuscated codes, which serve as toolkits used to exploit security holes, primarily within the browser, to further spread infection malware.



Mastering Your Introduction to Cyber Security

Michael C. Redmond, PhD
Lieutenant Colonel, USA, Retired
MBCP, FBCI, CEM, PMP

Certified as Lead Implementer:
ISO/IEC 27001 Information Security Management
ISO/IEC 27032 Lead Cyber Security Manager
ISO/IEC 27035 Security Incident Response

Certified as Lead Auditor:
ISO/IEC 27001 Information Security Management
ISO/IEC 22301 Business Continuity Management Systems

Cyber-attacks have increased exponentially, making this book essential in areas such as Business Management, Business Continuity and Disaster Recovery, Risk Management, Compliance, and IT. Dr. Michael C. Redmond, PhD takes a complicated subject and breaks it down into plain English...

Mastering Your Introduction to Cyber Security

by Dr. Michael C. Redmond PHD