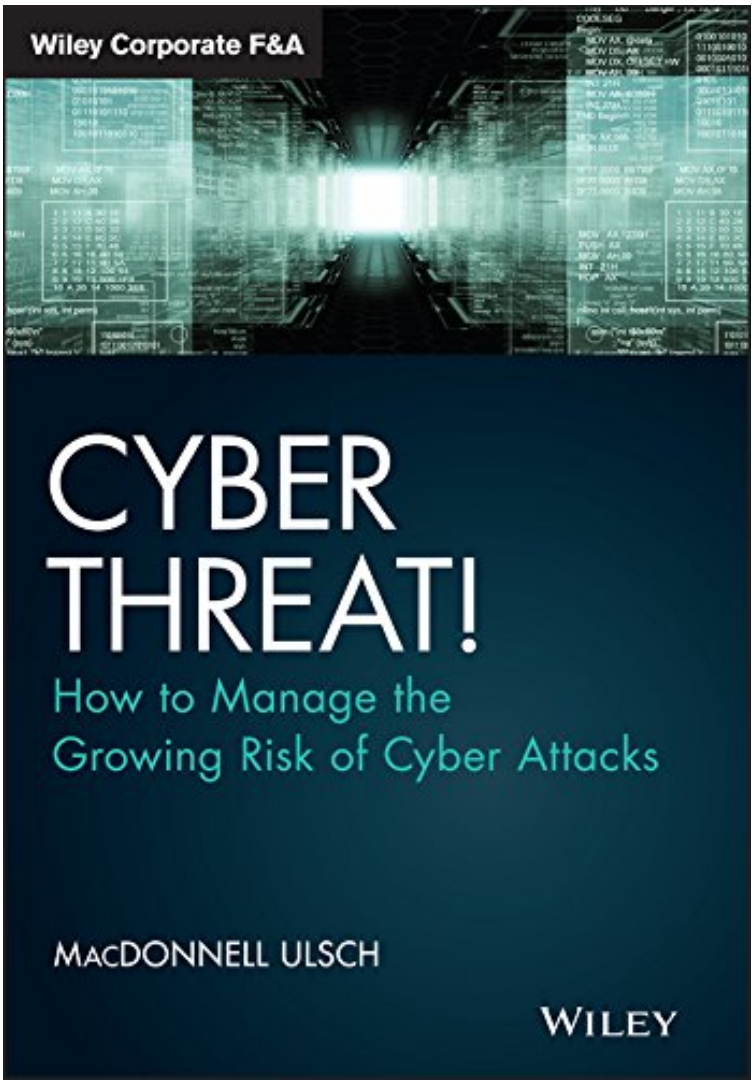
Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks (Wiley Corporate FA)

MacDonnell Ulsch
*audiobook | *ebooks | Download PDF | ePub | DOC*



#1528139 in eBooks 2014-07-14 2014-07-14File Name: B00JUUZXZI | File size: 41.Mb

MacDonnell Ulsch : Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks (Wiley Corporate FA) before purchasing it in order to gage whether or not it would be worth my time, and all praised Cyber Threat!: How to Manage the Growing Risk of Cyber Attacks (Wiley Corporate FA):

1 of 1 people found the following review helpful. Immediate Value for the C-Suite with Writing on the Wall for the UNBy JT JacobyUlsch unmasks the scale, politics, and velocity of cyber threats and then packages it into C Level readability; Irsquo;d rather read something memorable than something I have to memorize. He performs the necessary

navigation through typical cyber hazards like breach, bot nets, brand protection, APT, etc. However, unlike most literature on this topic, he also paints the bigger picture when he expands the dialogue from the true cost of a cyber-attack to ldquo;US Cyber Policyrdquo; to ldquo;Geopolitical Shiftsrdquo; which to me is most unsettling. Throughout the book he shows us that that China, nation states and organizations have clearly shunned outdated ICBMs and drones and opted for more helpful, and much cheaper, software based munitions. What about Stuxnet?Granted, we have our everyday jobs that demand prescriptive attention on what to do and there is solid direction in preparedness and response. However, if you want some how to book, this isnrsquo;t for you. Itrsquo;s helpful for executives who benefit from easier to recall snippets rather than minutia like percentage of global malware by originating country. Deeply technical information on cyber security is refreshed real-time on the web and if you want to learn how to do incident response pick up NIST SP800-61 as a primer.A great read for someone at a senior level who needs to get up to speed and ask the right questions. I hope his next book continues in both directions: working from the trenches and working from Brussels!Ulsch does present useful tools and approaches for your own shop as well as the less understood risks such as ldquo;The Emergence of the Cyber Nation Staterdquo; and ldquo;A Case of Cyber Espionage Conspiracy?rdquo; Itrsquo;s a clear call to action and Irsquo;d like to see more on that. Still, we have our everyday jobs that demand prescriptive attention on what to do. However, if you want some how to do book, this isnrsquo;t for you. Rather, itrsquo;s helpful for executives who benefit from easier to recall anecdotes rather than minutia like percentage of global malware by originating country. Irsquo;d rather read something memorable than something I have to memorize. Deeply technical information on cyber security is refreshed real-time on the web and if you want to learn how to do incident response pick up NIST SP800-61 as a primer.A great read for someone at a senior level who needs to get up to speed and ask the right questions. I hope his next book continues in both directions: working from the trenches and working on Brussels!2 of 3 people found the following review helpful. Good Content, Bad WritingBy Pizza QuixoteWhile the author is clearly expert, this is a scattershot book that is poorly written and not well organized. The wisdom in it could have been distilled into a much shorter book by a good editor. Hard to recommend, even though it contains several useful observations.2 of 4 people found the following review helpful. Five StarsBy Richard E. CrawfordAnother home run by Don Ulsch! Spot on!!

Conquering cyber attacks requires a multi-sector, multi-modal approach Cyber Threat! How to Manage the Growing Risk of Cyber Attacks is an in-depth examination of the very real cyber security risks facing all facets of government and industry, and the various factors that must align to maintain information integrity. Written by one of the nation's most highly respected cyber risk analysts, the book describes how businesses and government agencies must protect their most valuable assets to avoid potentially catastrophic consequences. Much more than just cyber security, the necessary solutions require government and industry to work cooperatively and intelligently. This resource reveals the extent of the problem, and provides a plan to change course and better manage and protect critical information. Recent news surrounding cyber hacking operations show how intellectual property theft is now a matter of national security, as well as economic and commercial security. Consequences are far-reaching, and can have enormous effects on national economies and international relations. Aggressive cyber forces in China, Russia, Eastern Europe and elsewhere, the rise of global organized criminal networks, and inattention to vulnerabilities throughout critical infrastructures converge to represent an abundantly clear threat. Managing the threat and keeping information safe is now a top priority for global businesses and government agencies. Cyber Threat! breaks the issue down into real terms, and proposes an approach to effective defense. Topics include: The information at risk The true extent of the threat The potential consequences across sectors The multifaceted approach to defense The growing cyber threat is fundamentally changing the nation's economic, diplomatic, military, and intelligence operations, and will extend into future technological, scientific, and geopolitical influence. The only effective solution will be expansive and complex, encompassing every facet of government and industry. Cyber Threat! details the situation at hand, and provides the information that can help keep the nation safe.

From the Inside FlapEveryone knows that information security is essential, yet there is never a shortage of news stories about large organizations suffering from cyber attacks. The disconnect lies in a lack of awareness about the real nature of cyber threats. Businesses fall victim to attacks because they think they are secure, failing to understand changing risks and emerging vulnerabilities. As MacDonnell Ulsch explains in Cyber Threat!, relying on outdated security strategies or on public policy is a dangerous game. Thankfully, minimizing corporate risk and protecting your brand are possible with the right knowledge and the ability to detect early warning signs. In Cyber Threat!, yoursquo;ll read about risk factors you may be overlooking, including many threats from inside that are easy and affordable to address. The abundant examples in this book make it all too clear that security breaches often go undetected for months and even years at a time. Thatrsquo;s because, even as threats intensify, risk remains inadequately assessed and awareness remains woefully low. These are problems that every organization should address right away. Cyber Threat! was written to guide that process with strategies for assessing risk and tips for managing your brand should an attack occur. Understanding the level of risk your organization faces requires knowing how your systems are

connected to the world of information. These connections are fundamentally changing the way the economy functions, and no one is immune. Cyber Threat! approaches the issue of information security from a one-of-a-kind global perspective. Because data can easily cross borders in the hands of cyber criminals, information security is a geopolitical issue. Internet-based organized crime, cyber activism hacking groups like Anonymous, and national strategies of cyber theft are all real threats to the technological infrastructure that businesses rely on. This book gives an eye-opening explanation of these complexities, providing readers with the global foundation they need to take action.From the Back CoverPraise for Cyber Threat! How to Manage the Growing Risk of Cyber Attacks ldquo;Don Ulsch is one of those rare cyber security experts who understands not only the technical issues involved in dealing with all manner of cyber threats and risks, but he also has an extraordinarily profound and visionary understanding of the face and future of cyber threats.rdquo; mdash;Anthony Kimery, Executive Editor, Homeland Security Today magazine ldquo;If you think cyber-security is someone elsersquo;s job, think again. This book makes the best case yet for why business executives need to sit up and take noticemdash;your companyrsquo;s future may depend on it.rdquo; mdash;Andrew Briney, Founding Editor, Information Security magazine ldquo;The author warns of threats, vulnerabilities, and reasons for action on the part of those responsible for safeguarding valuable assets against technological exploitation by adversaries. Executives, managers, security officers, and concerned citizens should follow this bookrsquo;s proper advice and guidance in order to manage ever-changing risks in a volatile cyber environment.rdquo; mdash;Maynard C. Anderson, Former Deputy Under Secretary of Defense (Security Policy) ldquo;Donrsquo;s book is a must-read for Corporate Executives and Directors to understand the broad implications of the cyber war being waged against American corporations. As one of the worldrsquo;s leading hands-on practitioners in the space, Don offers insightful guidance and proven mitigation strategies for firms to consider to protect your corporation and the interests of your shareholders from a menace likely to be with us for some time to come.rdquo; mdash;Thomas M. Wagner, Head of Business Continuity Management, The Direct Edge Stock Exchange, a BATS Global Markets Company ldquo;By using an exclamation point in the title of his book, Cyber Threat! How to Manage the Growing Risk of Cyber Attacks, Don highlights how critical cybersecurity is to every senior executive. Once the domain of those with specialized scientific and technical skills, the rise of the Advanced Persistent Threat coming from cyberspace means that this risk must be made part of any organizationrsquo;s management calculus and woe to the CEO who disregards its importance. Donrsquo;s book gives a clear and concise understanding that any executive can use to incorporate this risk management profile into their operational plans.rdquo; mdash;Kenneth P. Mortensen, former Associate Deputy Attorney General, Privacy Civil Liberties, U.S. Department of Justice ldquo;Businesses are now at grave risk from cyber-attacks that are being launched daily from all over the world by criminals, terrorists, and unfriendly nations. Don Ulsch has dedicated his life to understanding these threats, and Cyber Threat! is a clarion call to government and corporate leaders to recognize and tackle this virulent new form of warfare.rdquo; mdash;Col. James L. Bullion, Executive, U.S. Army, DoD (retired)About the AuthorMacDONNELL ULSCH is currently a managing director of cyber crime and breach response at a large international consulting firm. He is the author of the highly regarded book Threat! Managing Risk in a Hostile World. Mr. Ulsch has investigated many high-impact cyber breach and technology espionage cases and advises a diverse range of private-sector and government clients on the cyber threat, how to manage a cyber attack when it occurs, and how to reduce the risk impact of one. He has appeared on Fox News, ABC News, and other media outlets, and has been quoted in many publications, including academic and military studies.