cyber security business for sale

cyber security business for sale is a topic of growing interest among entrepreneurs and investors alike, as the demand for robust digital protection services continues to rise. With cyber threats becoming more sophisticated, businesses are increasingly seeking expert solutions to safeguard their data and systems. This article will explore the various aspects of purchasing a cyber security business, including the current market landscape, potential benefits, considerations before buying, and steps to take during the acquisition process. Additionally, we will discuss the types of cyber security businesses available and how to assess their value, ensuring you are well-informed before making a significant investment.

Understanding the Cyber Security Market

The cyber security market is a dynamic and rapidly evolving industry, driven by the increasing prevalence of cyber threats and the dire need for businesses to protect sensitive information. In 2023, the global cyber security market is projected to grow significantly, with estimates suggesting it could reach upwards of $300 billion by 2026. This growth is fueled by rising concerns over data breaches, ransomware attacks, and compliance requirements, creating a fertile environment for cyber security businesses.

Current Trends in Cyber Security

Several trends are shaping the cyber security landscape, making it an

appealing sector for investment:

- **Increased Regulatory Compliance:** Governments worldwide are implementing stricter data protection regulations, such as GDPR and CCPA, requiring businesses to adopt comprehensive security measures.
- **Adoption of Cloud Security Solutions:** As more companies migrate to the cloud, the demand for cloud security services is surging, leading to new opportunities in this niche.
- **Rise of Managed Security Service Providers (MSSPs):** Many businesses prefer outsourcing their cyber security needs, which has led to the growth of MSSPs that provide round-the-clock monitoring and support.
- **Focus on Threat Intelligence:** Organizations are increasingly investing in threat intelligence services to proactively identify and mitigate cyber risks before they escalate.

Benefits of Buying a Cyber Security Business

Investing in a cyber security business presents numerous advantages, especially in today's digital landscape where security threats are prevalent. Here are some key benefits:

Stable Demand for Services

The demand for cyber security services remains strong and is expected to grow. Businesses of all sizes require protection from various cyber threats, ensuring a steady stream of clients for a well-established cyber security firm.

Opportunity for Expansion

Purchasing an existing cyber security business provides an open door for expansion. You can leverage the existing client base, reputation, and infrastructure to introduce new services or enter new markets.

Access to Experienced Talent

Acquiring a cyber security business often means inheriting a skilled workforce. This experienced team can provide continuity and expertise, reducing the learning curve associated with starting a new venture from scratch.

Key Considerations Before Acquiring a Cyber Security Firm

Before making an acquisition, it's crucial to consider several factors that can influence the success of your investment.

Assessing Market Position

Evaluate the target company's position in the market. Analyze their reputation, client feedback, and overall service offerings to ensure they align with your business goals.

Financial Health of the Business

Conduct thorough due diligence to understand the financial health of the business. Review financial statements, profit margins, and the stability of client contracts to determine if the firm is a viable investment.

Legal and Compliance Issues

Ensure the business adheres to all legal and compliance requirements, as any oversight can lead to significant liabilities. Review any ongoing or past legal issues that might affect the acquisition.

Steps to Purchase a Cyber Security Business

Once you've decided to move forward with the acquisition, follow these key steps to ensure a smooth process.

Conduct Thorough Research

Begin with extensive research to identify potential targets. Utilize online platforms, business brokers, and industry connections to discover available cyber security businesses for sale.

Engage Professional Advisors

Consider hiring professionals such as business brokers, accountants, and legal advisors who specialize in mergers and acquisitions. Their expertise can guide you through the complexities of the acquisition process.

Negotiate the Terms

Once you've identified a target, engage in negotiations to agree on terms, price, and conditions of the sale. Be prepared to walk away if the deal does not meet your expectations or requirements.

Finalize the Acquisition

After negotiations, finalize the acquisition through a formal purchase agreement. Ensure all legal documents are properly executed, and conduct a final review to mitigate any risks associated with the acquisition.

Types of Cyber Security Businesses for Sale

Cyber security businesses come in various forms, each offering unique services and expertise. Understanding these types can help you identify the best fit for your investment goals.

Consulting Firms

These businesses provide expert advice on cyber security strategies, risk assessments, and compliance requirements. They typically work with various industries, offering tailored solutions.

Managed Security Service Providers (MSSPs)

MSSPs offer outsourced monitoring and management of security systems for businesses. They often provide 24/7 support, making them attractive to companies lacking in-house expertise.

Software Development Companies

Companies that develop security software, such as intrusion detection systems, antivirus programs, and firewalls, are also valuable acquisitions. Their proprietary technology can enhance your service offerings.

Assessing the Value of a Cyber Security Business

Determining the value of a cyber security business is crucial before making a purchase. Here are key factors to consider:

Revenue and Profitability

Analyze the business's revenue streams and profitability. Look for consistent revenue growth and a solid client base that contributes to financial stability.

Market Trends and Growth Potential

Evaluate current market trends affecting the cyber security industry. Consider the growth potential based on the target company's service offerings and market position.

Asset Valuation

Assess all tangible and intangible assets, including technology, intellectual property, and client contracts. These assets contribute significantly to the overall value of the business.

Conclusion

Investing in a cyber security business for sale presents a unique opportunity to enter a lucrative and essential market. With the increasing demand for cyber security services, understanding the landscape, assessing potential targets, and navigating the acquisition process is crucial for success. By conducting thorough research, engaging professional advisors, and carefully evaluating the opportunities available, you can position yourself to make a well-informed investment that enhances your portfolio and contributes to the ongoing battle against cyber threats.

Q: What should I consider when looking for a cyber security business for sale?

A: When searching for a cyber security business for sale, consider factors such as market position, financial health, legal compliance, and the skill set of existing employees. Conduct thorough due diligence to ensure the business aligns with your investment goals.

Q: What are the benefits of acquiring an existing cyber security firm?

A: Acquiring an existing cyber security firm provides immediate access to a client base, established reputation, experienced team members, and an opportunity for expansion into new services or markets.

Q: How can I assess the value of a cyber security business?

A: To assess the value of a cyber security business, analyze its revenue and profitability, evaluate market trends and growth potential, and conduct an asset valuation that includes both tangible and intangible assets.

Q: What types of services do cyber security businesses typically offer?

A: Cyber security businesses typically offer a range of services, including consulting, managed security services, software development for security applications, threat intelligence, and compliance management.

Q: What steps should I take to negotiate the purchase of a cyber security business?

A: To negotiate the purchase of a cyber security business, conduct thorough research on the target company, engage professional advisors, prepare a clear proposal, and be ready to negotiate terms that align with your financial objectives.

Q: Are there specific regulatory requirements for cyber security businesses?

A: Yes, cyber security businesses must comply with various regulatory requirements depending on their location and the industries they serve. Key regulations may include data protection laws like GDPR and industry-specific standards such as HIPAA for healthcare.

Q: How can I ensure a smooth acquisition process?

A: To ensure a smooth acquisition process, engage professional advisors, conduct comprehensive due diligence, maintain clear communication with the target company, and finalize all legal agreements meticulously.

Q: What is the role of Managed Security Service Providers (MSSPs)?

A: Managed Security Service Providers (MSSPs) offer outsourced monitoring and management of security systems, providing businesses with 24/7 support and expertise in preventing and responding to cyber threats.

Q: What trends are currently impacting the cyber security market?

A: Current trends impacting the cyber security market include increased regulatory compliance, the adoption of cloud security solutions, the rise of MSSPs, and a growing focus on threat intelligence services.

Cyber Security Business For Sale

cyber security business for sale: Enterprise Cybersecurity in Digital Business Ariel Evans, 2022-03-22 Cyber risk is the highest perceived business risk according to risk managers and corporate insurance experts. Cybersecurity typically is viewed as the boogeyman: it strikes fear into the hearts of non-technical employees. Enterprise Cybersecurity in Digital Business: Building a Cyber Resilient Organization provides a clear guide for companies to understand cyber from a business perspective rather than a technical perspective, and to build resilience for their business. Written by a world-renowned expert in the field, the book is based on three years of research with the Fortune 1000 and cyber insurance industry carriers, reinsurers, and brokers. It acts as a roadmap to understand cybersecurity maturity, set goals to increase resiliency, create new roles to fill business gaps related to cybersecurity, and make cyber inclusive for everyone in the business. It is unique since it provides strategies and learnings that have shown to lower risk and demystify cyber for each person. With a clear structure covering the key areas of the Evolution of Cybersecurity, Cybersecurity Basics, Cybersecurity Tools, Cybersecurity Regulation, Cybersecurity Incident Response, Forensics and Audit, GDPR, Cybersecurity Insurance, Cybersecurity Risk Management, Cybersecurity Risk Management Strategy, and Vendor Risk Management Strategy, the book provides a guide for professionals as well as a key text for students studying this field. The book is essential reading for CEOs, Chief Information Security Officers, Data Protection Officers, Compliance Managers, and other cyber stakeholders, who are looking to get up to speed with the issues surrounding cybersecurity and how they can respond. It is also a strong textbook for postgraduate and executive education students in cybersecurity as it relates to business.

cyber security business for sale: Cyber Security, Artificial Intelligence, Data Protection & the Law Robert Walters, Marko Novak, 2021-08-24 This book provides a comparison and practical guide of the data protection laws of Canada, China (Hong Kong, Macau, Taiwan), Laos, Philippines, South Korea, United States and Vietnam. The book builds on the first book Data Protection Law. A Comparative Analysis of Asia-Pacific and European Approaches, Robert Walters, Leon Trakman, Bruno Zeller. As the world comes to terms with Artificial Intelligence (AI), which now pervades the daily lives of everyone. For instance, our smart or Iphone, and smart home technology (robots, televisions, fridges and toys) access our personal data at an unprecedented level. Therefore, the security of that data is increasingly more vulnerable and can be compromised. This book examines the interface of cyber security, AI and data protection. It highlights and recommends that regulators and governments need to undertake wider research and law reform to ensure the most vulnerable in the community have their personal data protected adequately, while balancing the

future benefits of the digital economy.

cyber security business for sale: *Cybercrime and Business* Sanford Moskowitz, 2017-05-19 Cybercrime and Business: Strategies for Global Corporate Security examines the three most prevalent cybercrimes afflicting today's corporate security professionals: piracy, espionage, and computer hacking. By demonstrating how each of these threats evolved separately and then converged to form an ultra-dangerous composite threat, the book discusses the impact the threats pose and how the very technologies that created the problem can help solve it. Cybercrime and Business then offers viable strategies for how different types of businesses—from large multinationals to small start-ups—can respond to these threats to both minimize their losses and gain a competitive advantage. The book concludes by identifying future technological threats and how the models presented in the book can be applied to handling them. - Demonstrates how to effectively handle corporate cyber security issues using case studies from a wide range of companies around the globe - Highlights the regulatory, economic, cultural, and demographic trends businesses encounter when facing security issues - Profiles corporate security issues in major industrialized, developing, and emerging countries throughout North America, Europe, Asia, Latin America, Africa, and the Middle East

cyber security business for sale: Cyber Security & Digital Awareness Shruti Dalela, Mrs. Preeti Dalela, 2023-10-25 Cybersecurity and Digital Awareness for Students is an essential book designed for students pursuing various academic disciplines, such as BCA, BA, BCom, BTech, BHSc, and anyone looking to enhance their general awareness in the digital realm. This book combines comprehensive knowledge with a unique feature – multiple-choice questions (MCQs) to help students reinforce their learning. Key aspects of the book include: Cyber Threat Landscape: The book provides a clear understanding of the ever-evolving cyber threats, from malware and hacking to data breaches, making it relevant to students from diverse fields. Digital Literacy: Emphasizing the significance of digital literacy, it equips students with the knowledge needed to navigate and thrive in the digital world effectively. Data Protection and Privacy: In an era of data breaches and privacy concerns, the book educates students on safeguarding their personal information online and understanding relevant laws and regulations. Online Etiquette and Behavior: It delves into appropriate online conduct and addresses topics like cyberbullying and harassment, which are relevant to students in their personal and professional lives. Security Awareness and Education: The book encourages lifelong learning about emerging cyber threats and best practices for online safety, and it includes MCQs to reinforce this knowledge. Cybersecurity as a Career: It introduces the exciting field of cybersecurity as a potential career path, shedding light on various roles and the growing demand for cybersecurity professionals. Emerging Technologies: The book explores how cutting-edge technologies like artificial intelligence and the Internet of Things (IoT) are shaping the digital landscape and the importance of understanding their security implications. Global Perspectives: With a global outlook on cybersecurity, it highlights the international nature of cyber threats and the need to stay informed about worldwide trends. The MCQs interspersed throughout the book offer students the opportunity to test their comprehension and problem-solving skills. This book is a valuable resource for enhancing general awareness, preparing for future careers, and reinforcing knowledge about cybersecurity and digital awareness. It equips students to navigate the digital world confidently and responsibly, making it an invaluable addition to their educational journey.

cyber security business for sale: Cyber Security United States. Congress. Senate. Committee on the Judiciary. Subcommittee on Crime and Terrorism, 2011

cyber security business for sale: *Cybersecurity for Mango Man* Henry Harvin, 2023-10-04 First, the historical turning points in the development of the computer industry are examined in our book, with special focus on the dark side that saw the birth of worms, viruses, Trojan horses, and a threat environment that drove the need for a developing area of cybersecurity. Protective design objectives are used to describe our critical infrastructure protection and engineering design issues. For the preservation of national security concerns, a vigilant cyber intelligence capability is required

in order to handle cyber disputes and, more importantly, to prevent or combat cyberwarfare. Cyberspace and the cyber warfare environment must be taken into account in order to comprehend the components that make cyberwar viable in terms of both offensive and defensive operations.

cyber security business for sale: Cyber Security for Next-Generation Computing Technologies Inam Ullah Khan, Mariya Ouaissa, Mariyam Ouaissa, Zakaria Abou El Houda, Muhammad Fazal Ijaz, 2024-01-16 This book sheds light on the cyber security challenges associated with nextgeneration computing technologies, emphasizing the serious threats posed to individuals, businesses, and nations. With everything becoming increasingly interconnected via the Internet, data security becomes paramount. As technology advances, people need to secure their data communication processes. Personal data security, including data integrity and confidentiality, is particularly vulnerable. Therefore, the concept of cyber security forensics emerges to ensure data security for everyone, addressing issues such as data control, hijacking, and threats to personal devices such as mobile phones, laptops, and other smart technologies. This book covers key topics related to cyber security in next-generation computing technologies, ultimately enhancing the quality of life for citizens, facilitating interaction with smart governments, and promoting secure communication processes. KEY FEATURES Highlights innovative principles and practices using next generation computing technologies based cybersecurity Presents an introduction to recent trends regarding the convergence of AI/ML in cybersecurity Offers an overview of theoretical, practical, simulation concepts of cybersecurity

cyber security business for sale: Cybersecurity Harvard Business Review, Alex Blau, Andrew Burt, Boris Groysberg, Roman V. Yampolskiy, 2019-08-27 No data is completely safe. Cyberattacks on companies and individuals are on the rise and growing not only in number but also in ferocity. And while you may think your company has taken all the precautionary steps to prevent an attack, no individual, company, or country is safe. Cybersecurity can no longer be left exclusively to IT specialists. Improving and increasing data security practices and identifying suspicious activity is everyone's responsibility, from the boardroom to the break room. Cybersecurity: The Insights You Need from Harvard Business Review brings you today's most essential thinking on cybersecurity, from outlining the challenges to exploring the solutions, and provides you with the critical information you need to prepare your company for the inevitable hack. The lessons in this book will help you get everyone in your organization on the same page when it comes to protecting your most valuable assets. Business is changing. Will you adapt or be left behind? Get up to speed and deepen your understanding of the topics that are shaping your company's future with the Insights You Need from Harvard Business Review series. Featuring HBR's smartest thinking on fast-moving issues--blockchain, cybersecurity, AI, and more--each book provides the foundational introduction and practical case studies your organization needs to compete today and collects the best research, interviews, and analysis to get it ready for tomorrow. You can't afford to ignore how these issues will transform the landscape of business and society. The Insights You Need series will help you grasp these critical ideas--and prepare you and your company for the future.

cyber security business for sale: Cyber Security And Online Earning Ankesh Godbole , This Book Is About To Cyber Security Awareness And Online Earning.

cyber security business for sale: *National Cybersecurity and Critical Infrastructure Protection Act of 2014* United States. Congress. House. Committee on Homeland Security, 2014

cyber security business for sale: Cyber Security in Business Analytics Gururaj H L, B Ramesh, Chandrika J, Hong Lin, 2025-09-30 There is a growing need for insights and practical experiences in the evolving field of cyber security for business analytics a need addressed by Cyber Security in Business Analytics. Divided into sections covering cyber security basics, artificial intelligence (AI) methods for threat detection, and practical applications in e-commerce and e-banking, the book's team of experts provides valuable insights into securing business data and improving decision-making processes. It covers topics such as data privacy, threat detection, risk assessment, and ethical considerations, catering to both technical and managerial audiences. • Presents real-case scenarios for enhancing understanding of how cyber security principles are

applied in diverse organizational settings • Offers advanced technologies such as artificial intelligence methods for cyber threat detection, offering readers • Provides a detailed exploration of howAI can make cybersecurity better by helping detect threats, unusual activities, and predict potential risks • Focuses on the convergence of cyber security and data-driven decision-making and explores how businesses can leverage analytics while safeguarding sensitive information • Includes insights into cutting-edge techniques in the field, such as detailed explorations of various cyber security tools within the context of business analytics Cyber Security in Business Analytics will be useful for scholars, researchers and professionals of computer science and analytics.

cyber security business for sale: *Cyber Security and Law* Mr. Rohit Manglik, 2023-05-23 This book offers a detailed exploration of cyber security and law, focusing on key concepts, methodologies, and practical implementations relevant to modern engineering and technology practices.

cyber security business for sale: Cyber Security: Law and Guidance Helen Wong MBE, 2018-09-28 Implementing appropriate security measures will be an advantage when protecting organisations from regulatory action and litigation in cyber security law: can you provide a defensive shield? Cyber Security: Law and Guidance provides an overview of legal developments in cyber security and data protection in the European Union and the United Kingdom, focusing on the key cyber security laws and related legal instruments, including those for data protection and payment services. Additional context is provided through insight into how the law is developed outside the regulatory frameworks, referencing the 'Consensus of Professional Opinion' on cyber security, case law and the role of professional and industry standards for security. With cyber security law destined to become heavily contentious, upholding a robust security framework will become an advantage and organisations will require expert assistance to operationalise matters. Practical in approach, this comprehensive text will be invaluable for legal practitioners and organisations. It covers both the law and its practical application, helping to ensure that advisers and organisations have effective policies and procedures in place to deal with cyber security. Topics include: - Threats and vulnerabilities - Privacy and security in the workplace and built environment - Importance of policy and guidance in digital communications - Industry specialists' in-depth reports - Social media and cyber security - International law and interaction between states - Data security and classification - Protecting organisations - Cyber security: cause and cure Cyber Security: Law and Guidance is on the indicative reading list of the University of Kent's Cyber Law module. This title is included in Bloomsbury Professional's Cyber Law and Intellectual Property and IT online service.

cyber security business for sale: CYBER SECURITY BASIC 2023 CYBER SECURITY BASIC 2023, 2023-01-25 PROTECT YOUR FILES & DEVICES PROTECT YOUR WIRELESS NETWORK HOW TO PROTECT EQUIPMENT & PAPER FILES HOW TO PROTECT DATA ON YOUR DEVICES HOW TO PROTECT YOUR BUSINESS

cyber security business for sale: *Sales and Post-Sales Scripts for Cybersecurity Services* Vijay Martis, Sales and Post-Sales Scripts for Cybersecurity Services In today's digital landscape, where cyber threats loom large and data breaches can cripple organizations overnight, the role of cybersecurity professionals has never been more critical. But in a field dominated by technical expertise, the art of effectively selling and supporting cybersecurity services often takes a back seat. Enter Sales and Post-Sales Scripts for Cybersecurity Services – your comprehensive guide to mastering the human side of cybersecurity sales. This groundbreaking book bridges the gap between technical know-how and sales finesse, offering a treasure trove of strategies, scripts, and insights for cybersecurity sales professionals. Whether you're a seasoned expert or new to the field, this book will transform your approach to client interactions, helping you close more deals and build lasting relationships in the high-stakes world of cybersecurity. Dive into chapters that cover every aspect of the sales journey, from understanding client needs and crafting compelling pitches to overcoming objections and providing top-notch post-sales support. Learn how to translate complex technical jargon into value propositions that resonate with decision-makers. Discover techniques for building trust and rapport in an industry where trust is paramount. But this book goes beyond just

sales techniques. It emphasizes the importance of continuous learning and adaptation in the ever-evolving cybersecurity landscape. You'll gain insights into staying ahead of the curve, anticipating client needs, and positioning yourself as a trusted advisor in a rapidly changing field. With its friendly, conversational tone and wealth of practical examples, Sales and Post-Sales Scripts for Cybersecurity Services feels less like a textbook and more like a mentor guiding you through the intricacies of cybersecurity sales. Real-world scenarios and customizable scripts provide you with the tools to handle any sales situation with confidence. Moreover, this book recognizes that in cybersecurity, the sale is just the beginning. You'll learn strategies for excellent post-sales support, customer retention, and upselling – crucial skills for long-term success in this relationship-driven industry. Whether you're looking to boost your close rates, enhance your client relationships, or simply gain a competitive edge in the cybersecurity market, this book is your ultimate resource. It's not just about selling a product; it's about selling peace of mind in an increasingly uncertain digital world. Sales and Post-Sales Scripts for Cybersecurity Services is more than just a book – it's your partner in navigating the complex intersection of technology and human interaction. Arm yourself with the knowledge, skills, and confidence to excel in cybersecurity sales. Your clients – and the digital world – are counting on you.

cyber security business for sale: Cybersecurity Thomas A. Johnson, 2015-04-16 The World Economic Forum regards the threat of cyber attack as one of the top five global risks confronting nations of the world today. Cyber attacks are increasingly targeting the core functions of the economies in nations throughout the world. The threat to attack critical infrastructures, disrupt critical services, and induce a wide range of dam

cyber security business for sale: Security, Trust, and Regulatory Aspects of Cloud Computing in Business Environments Srinivasan, S., 2014-03-31 Emerging as an effective alternative to organization-based information systems, cloud computing has been adopted by many businesses around the world. Despite the increased popularity, there remain concerns about the security of data in the cloud since users have become accustomed to having control over their hardware and software. Security, Trust, and Regulatory Aspects of Cloud Computing in Business Environments compiles the research and views of cloud computing from various individuals around the world. Detailing cloud security, regulatory and industry compliance, and trust building in the cloud, this book is an essential reference source for practitioners, professionals, and researchers worldwide, as well as business managers interested in an assembled collection of solutions provided by a variety of cloud users.

cyber security business for sale: *What Every Engineer Should Know About Cyber Security and Digital Forensics* Joanna F. DeFranco, Bob Maley, 2022-12-01 Most organizations place a high priority on keeping data secure, but not every organization invests in training its engineers or employees in understanding the security risks involved when using or developing technology. Designed for the non-security professional, What Every Engineer Should Know About Cyber Security and Digital Forensics is an overview of the field of cyber security. The Second Edition updates content to address the most recent cyber security concerns and introduces new topics such as business changes and outsourcing. It includes new cyber security risks such as Internet of Things and Distributed Networks (i.e., blockchain) and adds new sections on strategy based on the OODA (observe-orient-decide-act) loop in the cycle. It also includes an entire chapter on tools used by the professionals in the field. Exploring the cyber security topics that every engineer should understand, the book discusses network and personal data security, cloud and mobile computing, preparing for an incident and incident response, evidence handling, internet usage, law and compliance, and security forensic certifications. Application of the concepts is demonstrated through short case studies of real-world incidents chronologically delineating related events. The book also discusses certifications and reference manuals in the areas of cyber security and digital forensics. By mastering the principles in this volume, engineering professionals will not only better understand how to mitigate the risk of security incidents and keep their data secure, but also understand how to break into this expanding profession.

cyber security business for sale: *The Internet Encyclopedia* Hossein Bidgoli, 2004 Publisher Description

cyber security business for sale: Cyber Security James A. Lewis, 2003-08-14 This volume looks at the challenges of cyberspace in an interdependent world and at the need for new, cooperative modes of governance to build cyber security. Making networks and critical infrastructure secure requires competent domestic strategies. But it also requires a willingness among governments to take the lead in supporting one another through effective legal structures and agreements such as the Council of Europe Convention on Cybercrime. The authors explore informal and formal bilateral and multilateral approaches to transnational cooperation on cyber security and examine the elements needed for success.--BOOK JACKET.

Related to cyber security business for sale

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees - Homeland DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees - Homeland DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees - Homeland DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees - Homeland DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

What is Cybersecurity? | CISA What is cybersecurity? Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality,

Home Page | CISA 4 days ago JCDC unifies cyber defenders from organizations worldwide. This team proactively gathers, analyzes, and shares actionable cyber risk information to enable synchronized,

Cybersecurity Best Practices | Cybersecurity and Infrastructure CISA provides information on cybersecurity best practices to help individuals and organizations implement preventative measures and manage cyber risks

Cybersecurity | Homeland Security 4 days ago The Department of Homeland Security and its components play a lead role in strengthening cybersecurity resilience across the nation and sectors, investigating malicious

Cybersecurity Training & Exercises | CISA Cybersecurity Exercises CISA conducts cyber and physical security exercises with government and industry partners to enhance security and resilience of critical infrastructure. These

Nation-State Threats | Cybersecurity and Infrastructure Security As the nation’s cyber defense agency and national coordinator for critical infrastructure security, CISA provides resources to help critical infrastructure and other stakeholders build resilience

Secretary Noem Terminates Inept FEMA Employees DHS Secretary Kristi Noem announced that she is firing two dozen members of FEMA's IT department after it was discovered that they brazenly neglected basic security

Strengthening America’s Resilience Against the PRC Cyber Threats As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure security and resilience, CISA’s mission is to safeguard America’s critical

Malware, Phishing, and Ransomware | Cybersecurity and - CISA Overview Cyber-attacks can come in many forms. Malware, Phishing, and Ransomware are becoming increasingly common forms of attack and can affect individuals

National Terrorism Advisory System Bulletin - Homeland Security Low-level cyber attacks against US networks by pro-Iranian hacktivists are likely, and cyber actors affiliated with the Iranian government may conduct attacks against US

Related to cyber security business for sale

RTX sells cybersecurity, intelligence business unit for $1.3 billion (C4ISRNET1y) A cashier at a Travelex Bureau de Change counts U.S. dollars in February 2004. (Ian Waldie/Getty Images) WASHINGTON — Defense company RTX said it's selling its cybersecurity business for $1.3 billion

RTX sells cybersecurity, intelligence business unit for $1.3 billion (C4ISRNET1y) A cashier at a Travelex Bureau de Change counts U.S. dollars in February 2004. (Ian Waldie/Getty Images) WASHINGTON — Defense company RTX said it's selling its cybersecurity business for $1.3 billion

Cyber security: What business leaders need to know about fiber internet connectivity (2d) For business leaders weighing the costs and benefits, Fiber Internet provides a stronger backbone for implementing end-to-end

Cyber security: What business leaders need to know about fiber internet connectivity (2d) For business leaders weighing the costs and benefits, Fiber Internet provides a stronger backbone for implementing end-to-end

Atos confirms it's negotiating sale of its cybersecurity business unit to Airbus (SiliconANGLE1y) The French aerospace industry giant Airbus SE is holding talks with its compatriot information technology firm Atos SE over buying its cybersecurity business unit, and has reportedly made an offer

Atos confirms it's negotiating sale of its cybersecurity business unit to Airbus (SiliconANGLE1y) The French aerospace industry giant Airbus SE is holding talks with its compatriot information technology firm Atos SE over buying its cybersecurity business unit, and has reportedly made an offer

RTX (Raytheon) to Sell its Cybersecurity Business for $1.3B (Homeland Security Today1y) The increased amount of time spent online due to COVID-19 restrictions, amongst other reasons, constitutes a risk factor in vulnerable individuals' potential pathway to extremism. (Europol) The

RTX (Raytheon) to Sell its Cybersecurity Business for $1.3B (Homeland Security Today1y) The increased amount of time spent online due to COVID-19 restrictions, amongst other reasons, constitutes a risk factor in vulnerable individuals' potential pathway to extremism. (Europol) The

Navigating AI-powered cyber threats in 2025: 4 expert security tips for businesses (ZDNet6mon) Cybercriminals are weaponizing artificial intelligence (AI) across every attack phase. Large language models (LLMs) craft hyper-personalized phishing emails by scraping targets' social media profiles

Navigating AI-powered cyber threats in 2025: 4 expert security tips for businesses (ZDNet6mon) Cybercriminals are weaponizing artificial intelligence (AI) across every attack phase. Large language models (LLMs) craft hyper-personalized phishing emails by scraping targets' social media profiles

Gartner: Three top trends in cyber security for 2024 (Computer Weekly1y) Security and risk management leaders face disruptions on multiple fronts: technological, organisational and human. Preparation and pragmatic execution are vital to address these disruptions and

Gartner: Three top trends in cyber security for 2024 (Computer Weekly1y) Security and risk management leaders face disruptions on multiple fronts: technological, organisational and human. Preparation and pragmatic execution are vital to address these disruptions and

Five Essential Steps To Land Your First Cyber Security Job (Forbes1y) As cyberattacks intensify, so does the demand for cybersecurity professionals. According to the 2023 Cyber Security Workforce Study by ISC2, one of the largest cyber security associations, roughly 4

Five Essential Steps To Land Your First Cyber Security Job (Forbes1y) As cyberattacks intensify, so does the demand for cybersecurity professionals. According to the 2023 Cyber Security Workforce Study by ISC2, one of the largest cyber security associations, roughly 4

NetApp Sets New Standard for Cybersecurity at the Storage Layer (Business Wire5mon) SAN JOSE, Calif.--(BUSINESS WIRE)--NetApp® (NASDAQ: NTAP), the intelligent data infrastructure company, today announced new data security capabilities that help customers strengthen their

cyber

NetApp Sets New Standard for Cybersecurity at the Storage Layer (Business Wire5mon) SAN JOSE, Calif.--(BUSINESS WIRE)--NetApp® (NASDAQ: NTAP), the intelligent data infrastructure company, today announced new data security capabilities that help customers strengthen their cyber

The UK's New Cyber Security Bill: A Call to Action for Tech Businesses (Infosecurity-magazine.com4mon) Recent weeks have seen cybersecurity thrown into sharp focus. Continuous cyber-attacks at key times of the year for businesses providing online services disrupts their own business as well as the

The UK's New Cyber Security Bill: A Call to Action for Tech Businesses (Infosecurity-magazine.com4mon) Recent weeks have seen cybersecurity thrown into sharp focus. Continuous cyber-attacks at key times of the year for businesses providing online services disrupts their own business as well as the

Back to Home: http://www.speargroupllc.com