

# Cybersecurity as a Strategic Opportunity



**DAVE CHATTERJEE, PH.D.**

Associate Professor, Terry College of Business,  
The University of Georgia, Athens, USA

Visiting Professor, Pratt School of Engineering,  
Duke University, Durham, USA

# Disclaimer



## **Fair Use Notice and Disclaimer**

This presentation deck may contain copyrighted material the use of which has not been specifically authorized by the copyright owner. The fair use doctrine allows the presenter limited use of copyrighted material without requiring permission from the rights holders, such as commentary, criticism, news reporting, research, teaching or scholarship. It provides for the legal, non-licensed citation or incorporation of copyrighted material in another author's work under a limited balancing test. The material shall be used to enhance public understanding of cybersecurity preparedness, as such, the presenter believes this constitutes a fair use of any such copyrighted material as provided for in section 107 of the US Copyright Law. In accordance with Title 17 U.S.C. Section 107, this presentation is distributed without profit to those who have expressed a prior interest in receiving the included information for research and educational purposes. If you wish to use potentially copyrighted material from this presentation for purposes of your own that go beyond fair use, you must obtain permission from the copyright owner.



## **Errors and Omissions Disclaimer**

The information contained in this presentation is for general guidance only. The author/presenter assumes no responsibility or liability for any errors or omissions in the content of this presentation. The information contained in this presentation is provided on an "as is" basis with no guarantees of completeness, accuracy, usefulness, or timeliness.

# Agenda

- 1 Relevant Professional Highlights
- 2 Cyber Risks and Vulnerabilities
- 3 Holistic Cybersecurity Governance Framework
- 4 Cybersecurity Strategic Capability Model
- 5 Closing Thoughts



# Relevant Professional Highlights



# Expertise and Roles

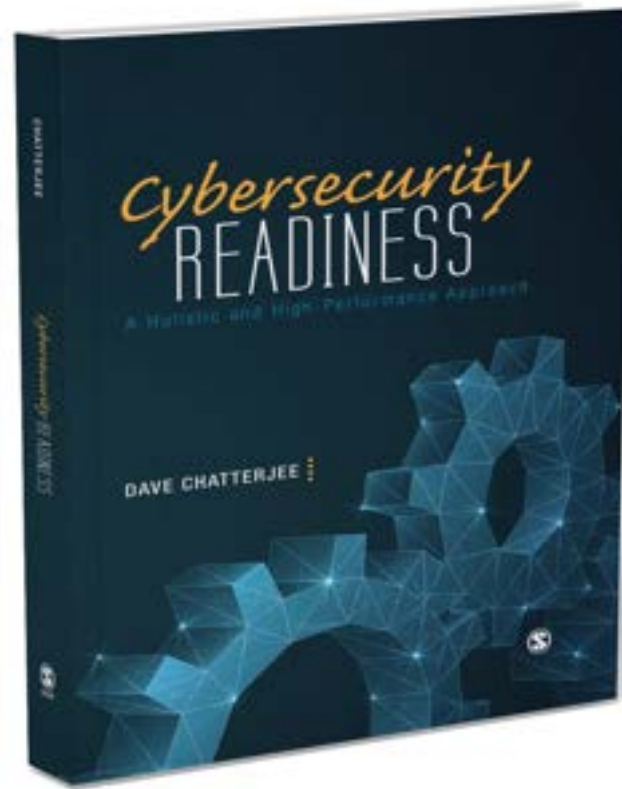
## Subject Matter Expertise

- Cybersecurity Governance
- Enterprise Digitization
- Strategic Management of Technologies

## Roles

- Professor
- Author
- Editor
- Speaker
- Consultant
- Strategic Advisor

# Cybersecurity Authorship



<https://www.amazon.nl/CYBERSECURITY-READINESS-Holistic-High-Performance-Approach/dp/1071837338>


# Cybersecurity Authorship

Harvard Business Publishing Education

Catalog ▾ Teaching Center ▾

---


---



 Article

**Calculated Risk? A Cybersecurity Evaluation Tool for SMEs**

*Michael Benz, Dave Chatterjee*

☆☆☆☆☆

 BUSINESS HORIZONS

 EDUCATOR COPY |  SHARE

**Calculated Risk? A Cybersecurity Evaluation Tool for SMEs, made the list of "Most Cited Articles since 2020," in Business Horizons**

# Cybersecurity Authorship

The screenshot shows the Harvard Business Publishing Education website. At the top left is the Harvard Business Publishing Education logo. To the right is a search bar with the placeholder text "Search for cases, simulations, and otl". Below the search bar are navigation links: "MY COLLECTIONS", "MY COURSEPACKS", "CATALOG", and "TEACHING SKILLS". The main content area features a blue square icon with a white book symbol and the word "Article" below it. To the right of the icon is the article title "Muddling Through Cybersecurity: Insights from the U.S. Healthcare Industry" in bold black text. Above the title is a small "Article" icon and a red "NEW" badge. Below the title is the author information "Chon Abraham, Dave Chatterjee, Ronald R. Sims" and a five-star rating system with five empty stars.

Harvard Business Publishing Education

Search for cases, simulations, and otl

MY COLLECTIONS MY COURSEPACKS CATALOG ▾ TEACHING SKILLS

Article **NEW**

**Muddling Through Cybersecurity: Insights from the U.S. Healthcare Industry**

*Chon Abraham, Dave Chatterjee, Ronald R. Sims*

☆☆☆☆☆



# Cybersecurity Authorship

Taylor & Francis Online

Journal  
**Journal of Organizational Computing and Electronic Commerce** >  
Volume 29, 2019 - Issue 1

Enter keywords, authors, I

854  
Views

1  
CrossRef citations  
to date

0  
Altmetric

Introduction


## Should executives go to jail over cybersecurity breaches?

Dave Chatterjee 

Pages 1-3 | Published online: 17 Feb 2019

 Download citation  <https://doi.org/10.1080/10919392.2019.1568713>  Check for updates

 Full Article  Figures & data  References  Citations  Metrics  Reprints & Permissions  Get acc

 Select Language | ▼  
Translator disclaimer

## ABSTRACT

The Consumer Data Protection Act, a new bill introduced by Senator Ron Wyden, is proposing "jail time of up to 20 years for executives who knowingly sign off on incorrect or inaccurate annual certifications of their companies' data-security practices." The bill also recommends that companies be fined "up to 4 percent of their annual revenue." While the critics consider the penalties too harsh and severe, the proposed legislation reflects two key realities – a) active involvement and commitment of

# Cybersecurity Authorship

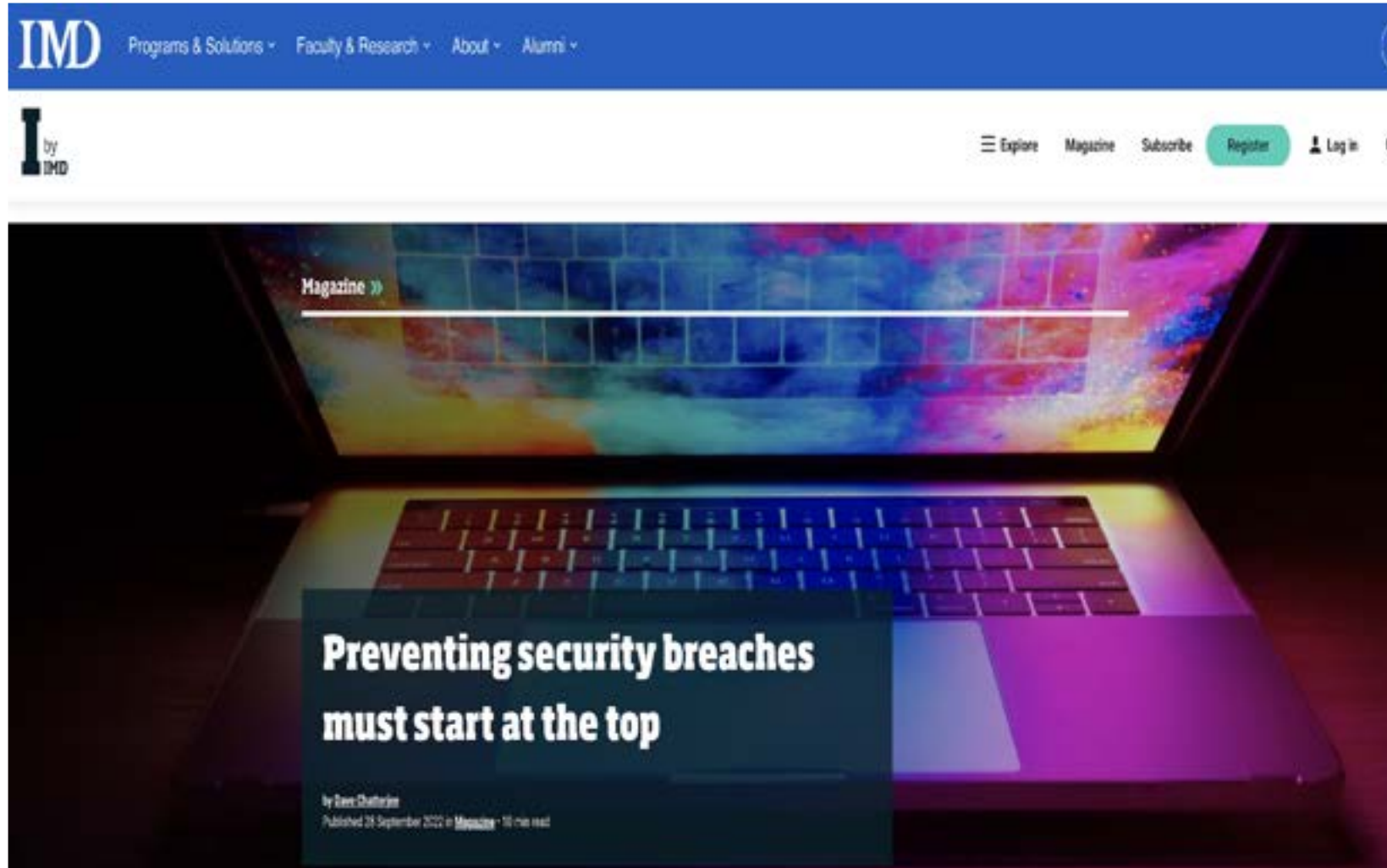
The image shows a screenshot of a website article. At the top, there is a blue navigation bar with the 'IMD' logo on the left and menu items: 'Programs & Solutions', 'Faculty & Research', 'About', and 'Alumni'. A search icon is on the right. Below this is a white navigation bar with the 'IMD by IMD' logo on the left and menu items: 'Explore', 'Magazine', 'Subscribe', 'Register' (in a teal button), 'Log in', and a search icon. The main content area features a large background image of a sunset over a field of clouds. A dark teal box is overlaid on the image, containing the following text:

Finance »

## Mission critical - How the American Cancer Society successfully and securely migrated to the cloud amid the pandemic

by Dave Chatterjee  
Published 13 March 2023 in [Essays](#) - 8 min read

# Cybersecurity Authorship



# Cybersecurity Readiness Podcast Series

Welcome to the Cybersecurity Readiness Podcast Site

The Cybersecurity Readiness P... Home Episodes About Contact Reviews + Q Follow

## Episodes

Search episodes...



April 24, 2021

### Developing Resilient and Secure Mission Critical Facilities (Data Cen...

Developing and maintaining resilient and secure data centers is a huge part of cybersecurity readiness. Spiros Lolis, Chief Technologist and Managing Consultant, EYP Mission Critical Facilities, Part of Ramboll, joins me to discuss the challenges and best practices of creating ...

[→ Episode page](#)



April 23, 2021

### Securing Application Programming Interfaces (APIs)

Application Programming Interfaces (APIs) play a vital role in modern software development, enabling the integration of services and facilitating the exchange of information. The ubiquity of APIs is a testament to their success in supporting many functions. However, their prominence ...

[→ Episode page](#)



March 27, 2021

### The Last Line of Defense Against a Ransomware Attack

Attackers have started increasingly targeting victims' backups to



March 18, 2021

### Overcoming the Stale Nature of Tabletop Exercises

While tabletop exercises (TTX) are considered a proven tool for finding gaps in an organization's security posture, they can be

Launched in June 2021  
Published 60 plus Episodes  
Listeners in 94 countries

<https://www.cybersecurityreadinesspodcast.com/>

Welcome to the Cybersecurity Readiness Podcast Site

The Cybersecurity Readiness P... Home Episodes About Contact Reviews + Q Follow

JAN, 18, 2021

## To trust or not to trust: the overwhelming challenge

News Social Share



Clinical psychologist Beatrice Cadet, Scientist Integrator at Netherland's Organization for Applied Scientific Research (TNO), draws upon multiple concepts such as 'learned helplessness' to explain why people still fall for phishing attacks despite the training. Beatrice emphasizes the need to factor in human behavioral traits and motivational triggers when developing social engineering solutions and training.



Show Notes

Clinical psychologist [Beatrice Cadet](#), Scientist Integrator at Netherland's Organization for Applied Scientific Research (TNO), draws upon multiple concepts such as 'learned helplessness' to explain why people still fall for phishing attacks despite the training. Beatrice emphasizes the need to factor in human behavioral traits and motivational triggers when developing social

Subscribe to gain more insight from the Cybersecurity Readiness Podcast!

Enter your first name...

Enter your email here...

I'm not a robot

By signing up, you agree to receive email from this podcast.

Subscribe

LISTEN ON

Apple Podcasts

Spotify

RSS Feed

RECENT EPISODES

The Last Line of Defense Against a Ransomware Attack

Overcoming the Stale Nature of Tabletop Exercises

Securing Artificial Intelligence (AI) Applications

Building a Resilient Disaster Recovery Infrastructure

Unraveling the Positive and Negative Impacts of Generative AI

Best Practices for Overcoming Troublesome Vulnerability Management Trends

Streamlining and Improving Security by Standardizing Identity Management

How Informed is the Board of Directors on Cybersecurity Risks?

# Cybersecurity Leadership Council & SWAT Team

## CYBERSECURITY COLLABORATIVE CORPORATE LEADERSHIP COUNCIL



**Jeanne Martin**  
Executive VP  
IT Risk & CRO  
IBM

**Marc Vanner**  
VP & Global CISO  
North America, IBM  
New York, NY

**Malcolm Harkins**  
Chief Security and Trust  
Officer  
Global Life

**Steve Young**  
Former CISO  
Blue Shield of California  
Berkeley

**Catharina "Di" Budharto**  
Sr. Director,  
Cybersecurity, Analytics  
& Data Protection  
Blue Shield of CA  
San Francisco



**Rich Anshur**  
CEO  
General Motors

**Tim Callahan**  
SVP & Global Chief  
Security Officer  
Alltel

**Mike Wilson**  
SVP and Chief Security  
Officer  
Wells Fargo

**Kim Owen**  
Senior CISO  
Chesapeake

**Nikolay Chernavsky**  
SVP & CISO  
Roughly



**Stan Lowe**  
Global CISO  
Zurich

**Jim O'Connor**  
CISO  
Cargill

**Joe Ellis**  
VP & CISO  
Roper Systems, Inc.

**Linda Dawson**  
Former Jackson &  
Levy/Johnson & Johnson  
San Francisco

**John Bingham**  
Global CISO  
Genentech, Sanofi  
San Francisco



**David Orsz**  
VP and CISO  
Bank of America

**George Manopakis**  
Sr. Director of Information  
Security  
Microsoft/Citigroup

**Adam Fletcher**  
CISO  
The Business Group  
Washington, DC

**Mark J. Viola**  
VP & Global CISO  
Hershey Foods Co.



**Dave Chatterjee**  
World-Renowned Technology  
Thought Leader and Business  
Strategist  
The University of Georgia



**Mark Chiock**  
Partner and Former Global CISO  
Submarine

## CYBERSECURITY COLLABORATIVE COMMUNITY LEADERSHIP COUNCIL



**Kiersten Todd**  
Managing Director  
Cyber Resilience Institute

**Dave Chatterjee**  
World-Renowned  
Technology Thought  
Leader and Business  
Strategist  
The University of Georgia

**Daniel Eliot**  
Director of Small  
Business Education  
National Cyber Security  
Alliance

**Laszlo Gerc**  
Co-founder and  
Managing Partner  
Next Era Transformation  
Group

**Teri Takai**  
Executive Director,  
Center for Digital  
Government  
ES&S/IS



**Leslie Kesselring**  
Founder and President  
Rising  
Communications

**Philip Kagan**  
CISO  
Girl Scouts of the USA

**Dan Gorecki**  
SVP Information  
Security  
Avaya

**Bryan Hurd**  
VP  
Steelcase/Johnson  
Johnson

**Kimberly Owen**  
Interim CISO  
ChargePoint, Inc.



**Juancarlos Martinez**  
VP Information  
Security Manager  
Columbia Bank

**Mike Dooley**  
Information Security  
Officer  
Veeva

**Christopher Vestch**  
Partner  
PricewaterhouseCoopers

**Jason Edwards**  
Compliance Director-  
Information  
Security/Cyber Security  
USA

**Griffin Weaver**  
Technology and  
Outsourcing Counsel  
USA



**Terry Waters**  
Independent  
Consultant  
Mikens Advisory



**Layton Holcombe**  
Director of Global  
Cyber Security Talent  
Network  
Alston, Todd, Baker LLP



**Jim Rutt**  
Chief Information  
Officer  
Dana Foundation

# Talks & Webinars

ISACA South Florida 2018 Annual General Meeting with Dr. Dave Chatterjee @ Renaissance Hotel / ISACA South Florida Chapter



Home About Certifications News Events Resources Careers Galleries Contact

## ISACA South Florida 2018 Annual General Meeting with Dr. Dave Chatterjee @ Renaissance Hotel

by Alicia Perdomo-Silvestre



The guest speaker at this year's Annual General Meeting being held on May 10th 2018 @ Renaissance Hotel Plantation Florida is [Dr. Dave Chatterjee](#)

Topic: **Life Aboard A U.S. Nuclear Submarine: What Has That Got To Do With Cyber Security?**

How does an organization earn and maintain customer trust amid growing concerns of data IT safety and security? The overall goal is to help firms become and remain highly reliable.

Life aboard a nuclear submarine is rough. A recent article on the just launched USS South Dakota describes how 135 sailors have to take turns sleeping, as there are only 34 beds. Space is at a premium on this high-tech vessel with the dining room doubling up as an operating theater, and the torpedo room becoming the exercise and sleeping area. Getting used to a life of indistinguishable night and day, working and sleeping at odd hours, learning to make your way through narrow walkways without running into others, and maintaining a quiet and peaceful environment is not easy.

It also requires great discipline and loyalty to strictly follow protocols and procedures that govern behavior during and after work hours. The service personnel operate in a culture of high-performance expectations where mistakes and failures can be catastrophic. Admiral Hyman Rickover, the Father of the US Nuclear Navy, is credited with creating and sustaining such a high-reliability organization (HRO) that has an exemplary zero-failure track record over its sixty-plus year existence.

<http://isacsf.org/2018agm/>

1/1



## Life Aboard A U.S. Nuclear Submarine : What Has That Got To Do With Cyber Security Best Practices?

ISACA South Florida Chapter

May 10, 2018

**Dr. Dave Chatterjee**

Associate Professor, The University of Georgia

Senior Editor, Journal of Organizational Computing and Electronic Commerce

Collaborating Researcher, Innovation Value Institute, Maynooth University, Ireland

# Talks & Webinars



UNIVERSITY OF ILLINOIS | SPRINGFIELD

## Cybersecurity Readiness:

A Holistic and High-Performance Approach

**Dr. Dave Chatterjee**

**March 25, 2022**  
**6 to 7 p.m.**  
Student Union Ballroom

The College of Business and Management at the University of Illinois Springfield hosts Dr. Dave Chatterjee to discuss how organizations need a comprehensive cybersecurity plan that requires execution with great precision and consistency.

Dr. Dave Chatterjee, Ph.D., is tenured professor in the Management Information Systems (MIS) at the Terry College of Business, The University of Georgia. His highly endorsed book, *Cybersecurity Readiness: A Holistic and High-Performance Approach*, was published by SAGE Publishing in March 2021. Dr. Chatterjee is also the host of Cybersecurity Readiness Podcast Series.

This event is made possible thanks to a gift from Louis and Christine Friedrich as part of the CSMY Business and Society project.



teissTalk  
Cracking Cyber Security

Tuesday, 10 May 2022 | 16:00 (BST)

### Designing threat resilient organisations

Panelists: Jenny Black (Host), Dr. Dave Chatterjee (University of Georgia and Visiting Scholar, Duke University), Vlad Brankic (Chief Information Security Officer, OFC Business Group), Michelle Griffin (Chief Risk Officer, CommBank)

Opening Guest, teissTalk LIVE Event  
May 10, 2022



COMPUTING AND ELECTRONICS RESEARCH SUMMIT 2022

ALL GUEST LECTURES  
30th - 31st March 2022

Panelist: Dr. Dave Chatterjee

Panelist, Computing and Electronics Research Summit, BITS Pilani  
March 31, 2022



NABIL HANNAN      DAVE CHATTERJEE

## AGENT OF INFLUENCE

A NetSPI Podcast | Hosted By Nabil Hannan

NetSPI Agent of Influence, Podcast Guest  
Sept. 2021



CIRCADENCE LIVE WEBINAR

TEACHER 2 TEACHER

### Cyber Training Done Right:

Teaching Technical and Non-Technical Skills to Prepare the Future Workforce

MAY 18<sup>th</sup> 9AM PST - 9AM MST - 11AM EST

Panelists: Dr. Dave Chatterjee, Dr. Brad Hayes

Project Ares by Circadence  
Webinar, May 2021

# Talks & Webinars



**UNC-Chapel Hill World View  
Conference, Nov 2022**



**18th European Conference on  
Cyber Warfare and Security, July  
2019**



**London School of Economics,  
Feb 2020**



**The European Information Security Summit,  
Feb 2020**



# Expert Interviews



**PRO Business Channel**



**National Public Radio/WABE 90.1**



**AIB TV Network**



**Guest, 'Ask The Expert,' Red Sift**

# Teaching and Workshops

## Learning Goals

- Understand the different types of information security vulnerabilities and challenges that plague organizations.
- Recognize the various people, process, and technology driven information security defense mechanisms and best practices.
- Evaluate the robustness and maturity of a cybersecurity program.
- Develop a defense in-depth information security strategy.
- Understand the implications of cybersecurity and privacy laws and regulations.
- Apply cybersecurity readiness assessment tools.
- Develop an information security control monitoring program.
- Evaluate the performance of a cybersecurity program.

## Course Highlights

### Holistic and Comprehensive Insight

- Into the different aspects of cybersecurity program management

### Highly Interactive and Hands On

- Instructor and student led class discussions
- Cyber Attack simulation activity
- Case Analyses
- Real world Project
- Security Information and Event Management Tool demo
- Immersive and Gamified Cybersecurity Training Platform demo

### Guest Speakers

- Subject Matter Experts from USA, United Kingdom, France, and Ireland

## Course Material

### Textbook Authored by Course Instructor

- [Cybersecurity Readiness: A Holistic and High-Performance Approach](#)

### Learning Resources at No Cost to Students

- Readings
- [Cybersecurity Readiness Podcast Episodes](#) (hosted by Dr. Chatterjee)
- Cyber Attack Simulation Tool

## CYBERSEC-521

### CYBERSECURITY PROGRAM DEVELOPMENT, OPERATIONS & ANALYSIS

#### When:

Mondays 8:30 - 11:15 AM  
Course begins Wednesday, January 9th, 2022

#### Who:

Professional, graduate, and undergraduate students from any discipline/field. No Prerequisites Required!

#### Why:

"Cybersecurity readiness is everyone's business."

#### Instructor:

**Dave Chatterjee, Ph. D.**

<https://dchattie.com/>  
<https://cybersecurity.meng.duke.edu/faculty/dave-chatterjee>

## Program Overview

The CISO Executive Education Program is managed by the [Duke Master of Engineering in Cybersecurity](#) in collaboration with [Duke Sanford School of Public Policy](#), the [Duke Law School](#), and the [Department of Computer Science](#). The collective expertise of these units and key industry partners offers a comprehensive and interdisciplinary framework, enabling the effective management and leadership of cybersecurity teams. When program participants finish this program, they will be able to:

- Provide *oversight and governance* for a cybersecurity program.
- Develop *cybersecurity metrics* that align to organizational goals.
- Identify *regulatory or legal risk* to the organization.
- Identify *goals for high performance* cybersecurity operations teams.
- Understand *emerging technologies and potential risk* impact to the organization.

### Week 1

*In-person, four-day intensive immersion during the [Cybersecurity Leadership Program](#)*

### Weeks 2 - 10

*Weekly virtual modules, each consisting of 3 hours of instruction*

### Week 11

*Final Examination*

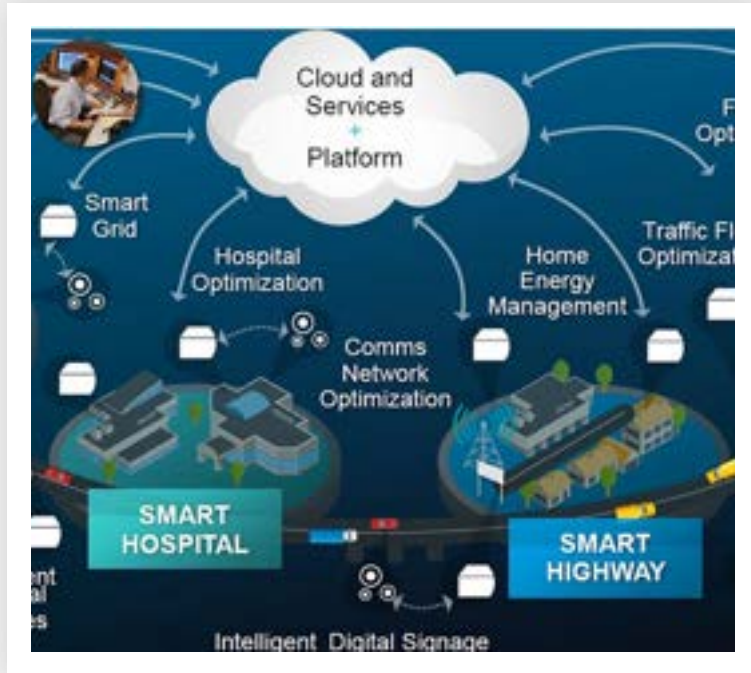
# USA TODAY – April 8, 2024

The image shows a screenshot of a USA TODAY article. At the top, there is a navigation bar with the USA TODAY logo on the left and several menu items: 'TRUMP ASSOCIATED TROUBLES' with a sub-item 'Aides in court', 'TAYLOR SWIFT NEWSLETTER: SIGN UP!' with a sub-item 'This Swift Beat', 'SOMETHING ON YOUR MIND?' with a sub-item 'Submit a column', 'ASAP TO SIGN' with a sub-item 'National parks guide', and 'SUBSCRIBE NOW \$3 for 1 year'. Below the navigation bar is a secondary menu with categories: 'U.S.', 'Elections', 'Sports', 'Entertainment', 'Life', 'Money', 'Tech', 'Travel', 'Opinion', a search icon, '53°F', a weather icon, a 'Subscribe' button, and a 'Sign In' dropdown. The main content area has a 'CONTRIBUTOR CONTENT' label above the article title. The title is 'Dave Chatterjee Drops the Cybersecurity Jargon, Encouraging Proactiveness Rather than Reactiveness'. Below the title is the author's name 'Tyler Shepherd Contributor' and the publication date 'Published 1:44 p.m. ET April 8, 2024'. There are social media sharing icons for Facebook, X, and Email. The article text begins with 'Cybersecurity, a term often used lightly, seldom understood, and frequently understated, has entered the public sector without warning, confusing many business owners and inexperienced individuals. While adequate mainstream implementation of cybersecurity still has a long way to go, with only 40% of business leaders believing cybersecurity threats will highly affect the organization's performance, the impact of security breaches can't be ignored, calling for immediate action, education, and widespread awareness.' The second paragraph states 'According to recent statistics published by Forbes, there were 2,365 cyberattacks in 2023, affecting over 343 million victims. Last year also saw a 72% increase in data breaches since 2021. The most common malware method was executed via email (35% of all breaches), and a staggering 94% of companies have reported email security issues. If successful, a cyberattack costs an organization \$4.45 million on average, posing a significant threat to companies worldwide, specifically small and medium ones.' The third paragraph starts with 'While cyberattacks are undeniably one of the most prominent threats modern-day companies face, many business leaders undermine the far-reaching consequences of insufficient security systems. Dr. Dave Chatterjee, a Cybersecurity and Technology Expert, an Associate Professor at the University of Georgia, a visiting Professor at Duke University, and a fervent advocate of competent security measures, has devoted his career to spreading awareness about the threats of cyberattacks and data breaches, empowering businesses to take an educated proactive stance.'

# Cyber Risks and Vulnerabilities



# Expanding Attack Surfaces



Digitization of processes



A highly mobile work environment



Increasing dependence on cloud-based services



Infusion of IoT and other smart devices

# Major and Evolving Attack Vectors



Phishing



Ransomware



IoT Attacks



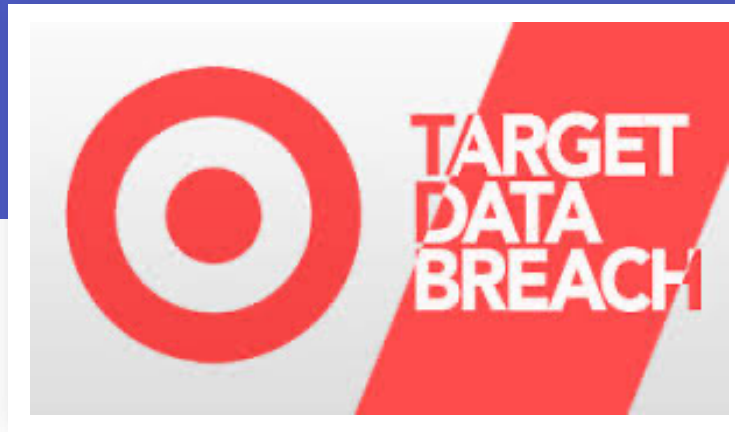
Insider Threats



Adversarial AI Attacks



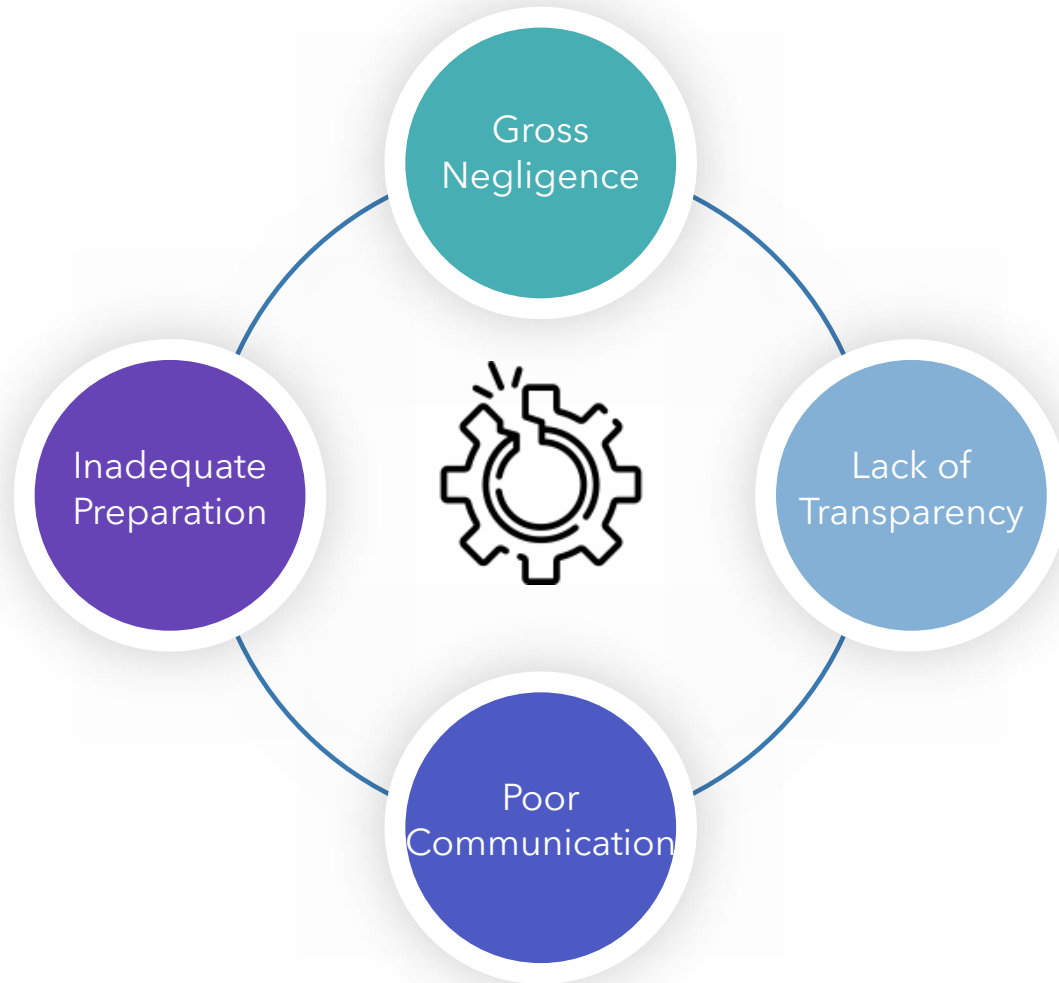
# The Human Vulnerability Factor



90%

of the attacks are focused on exploiting human vulnerabilities

# Common Weaknesses and Shortcomings



- Usernames and Passwords not encrypted
- Weak encryption system
- Unencrypted customer data stored in multiple locations
- Networks not adequately segmented
- Multi-factor Authentication (MFA) not in place
- Delay in notifying victims
- The breach went undetected for several weeks.
- The company did not pay heed to the alerts sent by the monitoring company.
- Misconfigured web application firewall
- Lack of well rehearsed disaster recovery and incident response plan

Based on the review of data breach records during the period 2010-2023



# The Critical Need

Cybersecurity  
governance  
needs to:

Shift from reactive to proactive mode

Go beyond regulatory compliance

Be more than check-the-box

Create and sustain a high-performance information  
security culture

# Holistic Cybersecurity Governance Framework



# Commitment-Preparedness-Discipline Framework



Source: Chatterjee, D. Cybersecurity Readiness: A Holistic and High-Performance Approach, SAGE Publishing, March 2021

# Commitment-Preparedness-Discipline Framework



# Commitment-Preparedness-Discipline Framework



Source: Chatterjee, D. Cybersecurity Readiness: A Holistic and High-Performance Approach, SAGE Publishing, March 2021

# Distinctive Characteristics



## **Holistic Approach**

Technology alone will not mitigate information security risks.

There are several pieces to the complex puzzle of cybersecurity management and technology is only one of them.

Other success factors include committed leadership, robust governance procedures, and informed and motivated personnel.

## **Proactive, Long-Term, and Sustainability-Focused Approach**

Creating and sustaining a high-performance information security culture is key to helping organizations stay committed to their cybersecurity goals and operate at a high level of efficiency and effectiveness for a sustained period.

## **Research-Driven Approach**

Extensive research and analyses led to the identification of seventeen success factors that are associated with three cultural dimensions: Commitment, Preparedness, and Discipline

# Distinctive Characteristics

- Pragmatic and Comprehensive Guide
- Intuitive and Easy to Follow
- Guiding Questions for reflection, self-assessment, and validation
- Numerous Vignettes and Cases to illustrate the applicability and value of the framework
- Cybersecurity Readiness Scorecards - An Organizational Self-Assessment Tool



# Methodology

- Data was gathered from primary and secondary sources.
- A multi-method approach of literature review, focus groups, and expert interviews was used to collect data.
- In-depth interviews with business leaders and subject matter experts were important sources of insight.
- The interviewees belonged to for-profit and non-profit organizations representing a wide range of industries:
  - Higher educational institutions
  - Government agencies
  - Information technology services
  - Healthcare
  - Financial technology (fintech)
  - Insurance services
  - Security and information management solutions
  - Food and beverages
  - Communications and information technology
- Qualitative tools and techniques were used to analyze the data.





# Cybersecurity Strategic Capability Model



# Cybersecurity Strategic Capability Model



**Cybersecurity Competencies**

- Proactiveness
- Resiliency
- Transparency
- Robustness
- Awareness



**Strategic Capabilities**

- Brand Reputation Management
- Secure Product/Service Management
- Customer Relationship Management
- Partner Relationship Management



**Strategic Outcomes**

- Revenue Growth
- Market Share Growth
- Realize Cost Efficiencies

Commitment-Preparedness-Discipline Framework

# Hands-On Top Management

## Mindset Shift

- Treat cybersecurity challenges as a strategic opportunity
- Treat cybersecurity capabilities as core competencies

## Active Engagement

- In all aspects of cyber governance - from strategizing to monitoring and measurement
- Take ownership and responsibility
- Serve on governance teams
- Participate in training and awareness programs

“Several of us in senior leadership are digital immigrants and not digital natives. Many of the security issues are new to us. We will be naïve if we don't take interest and are not willing to learn and stay updated.



# 'We-Are-In-It-Together' Culture

## Multi-pronged approach



Creating awareness



Building emotional capital (among employees and business partners)

- Feeling valued
- Developing a sense of belonging
- Taking pride in their work
- Having fun
- Perceiving leadership to be genuine and authentic



Incentivizing behavior

**Source:** Chatterjee, D. Cybersecurity Readiness: A Holistic and High-Performance Approach, SAGE Publishing, March 2021



# Joint Ownership and Accountability



WHO IS  
ACCOUNTABLE



“Business partners, third party service providers,  
and vendors must share responsibility in  
protecting sensitive data”

# CISO Empowerment

- CISO must be appropriately empowered to be effective
- Ideally, the CISO should be part of the C-level team or at least have direct access to the top management

“

There is growing recognition that the CISO is much more than a risk or technology officer. They are business enablers and must be involved in strategic and value creation activities



# Sustainable Budget



The funding must be sustained over the long-term, as it takes time to build robust defense capabilities.



Must be treated as strategic investments

# Comprehensive Asset Discovery

- The Cybersecurity and Infrastructure Security Agency recently issued a directive (BOD 23-01) requiring federal enterprises (civilian executive branch) to perform automated asset discovery every 7 days.

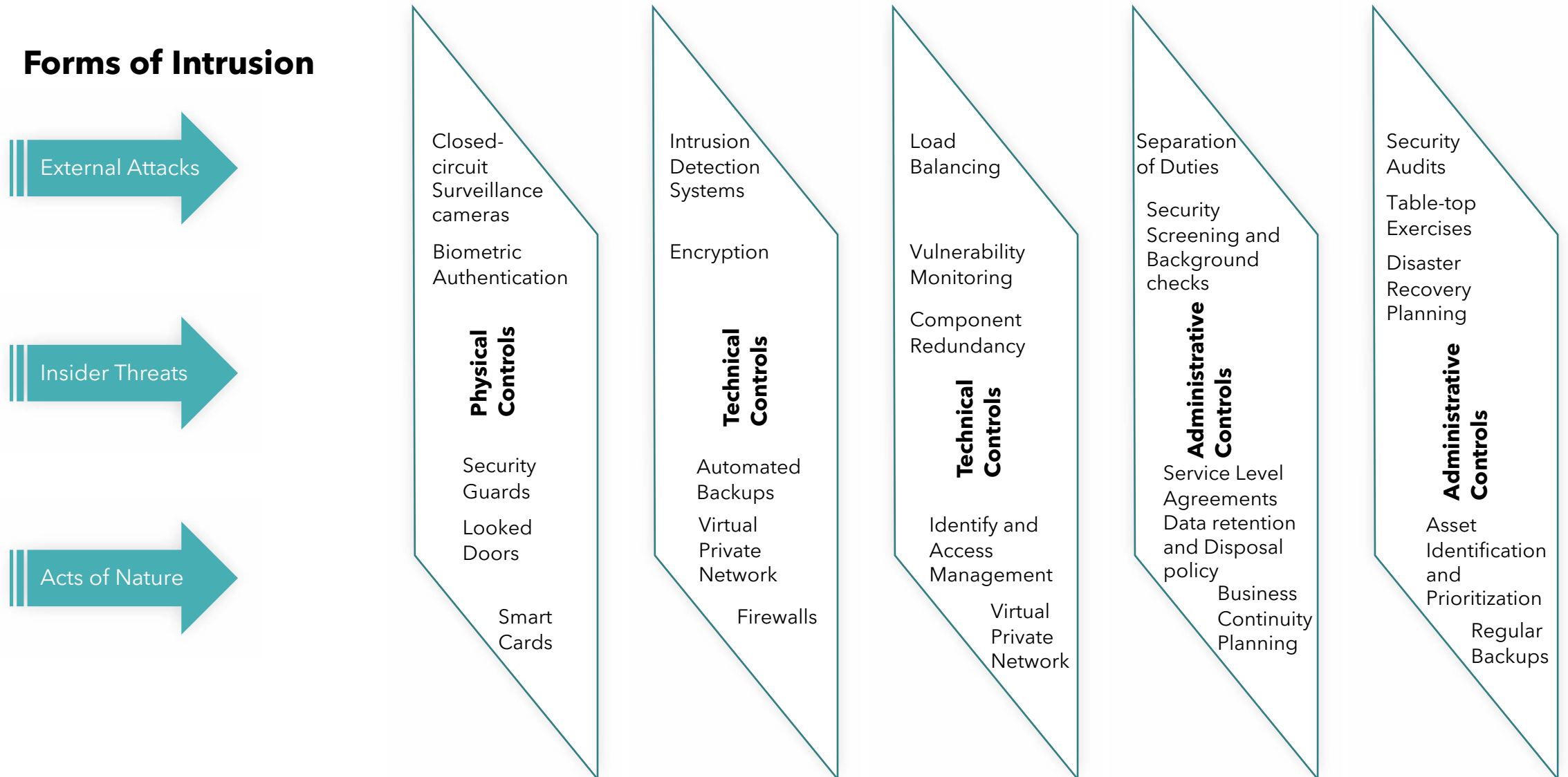
“

There are many hurdles associated with asset inventory management. The one that looms the largest is unmanaged devices, unmanaged assets, the Achilles heel of any asset inventory program.





# Defense-in-Depth Approach



# Role-Based Awareness and Training

01

Role-based

02

Incremental and continuous

03

Engaging and interactive

04

Important component of performance review

Like Wordle and Nerdle, the daily word and mathematics games and challenges, organizations can adopt an incremental and continuous approach to spreading security awareness and knowledge.

# Robust Data Backup and Retention Strategy



Method and frequency of data backup should be carefully determined and closely followed.

- Differential Backup
- Incremental Backup
- Full Backup



Create a backup of backups and make them “read-only.”



Having immutable backups that are encrypted.



Data should be backed up in both online and offline storage locations.



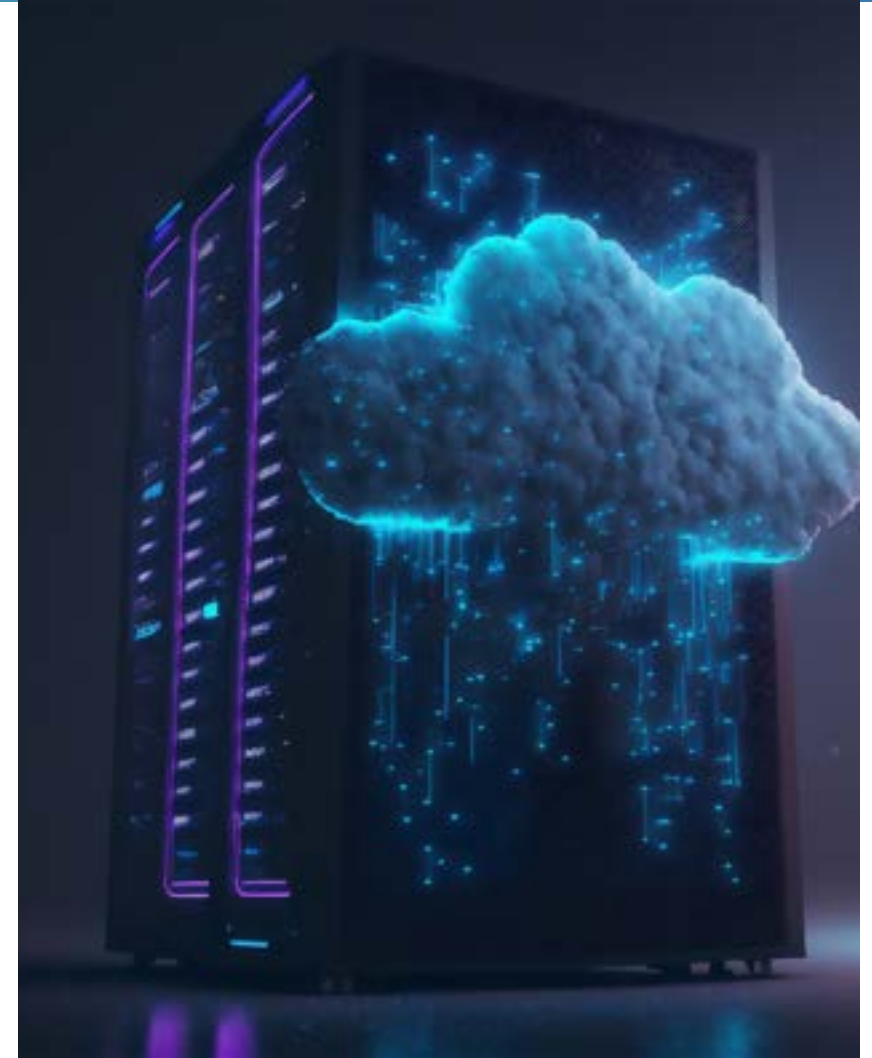
The data restoration process should be tested frequently.



Data storage and deletion policies should be determined based on a careful review of regulatory guidelines.



Service level agreements (SLAs) with managed service providers must clearly spell out data backup, storage, and purge provisions.



# Continuous Monitoring & Prompt Action



Formulation and documentation of continuous monitoring strategy



Establishing monitoring schedule



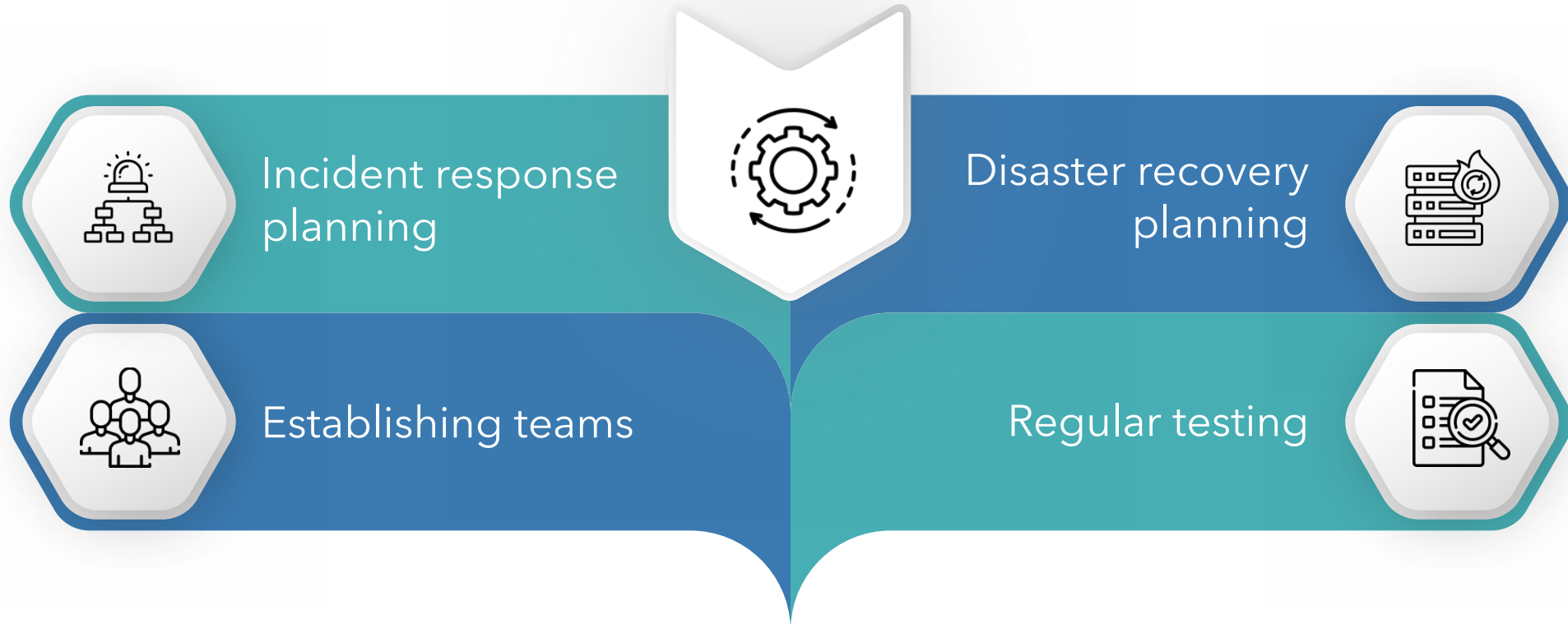
Use of automated vulnerability scanning tools



Prompt communication and action

**Thorough logging of monitoring results, actions taken, and decision-making rationale.**

# Highly Rehearsed Response & Recovery Capability



# Real-Time Security Audits and Drills

Regular security audits and drills



Real-time security audit

Conduct security drills to test recovery capability

# Closing Thoughts



# Ideal Mindset and Approach

## Mindset



Consider the cyber attack epidemic to be a strategic opportunity



Treat cybersecurity as a strategic competency/capability



Everyone has a role to play in securing the organization





# Ideal Mindset and Approach

## Approach



Be proactive



Be prepared



Continuously monitor and make adjustments



Promptly act on the intelligence received



Continuous training



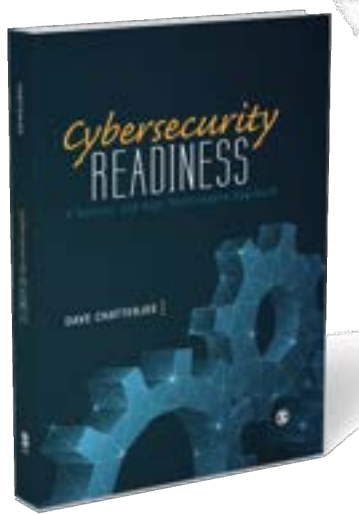
Don't outsource cybersecurity governance;  
actively engage and manage



Be truly committed to protecting  
confidential and strategic assets



Go above and beyond the Check-the-  
Box approach



# THANK YOU!!



## Book

Cybersecurity Readiness: A Holistic and High-Performance Approach



## Podcast

The Cybersecurity Readiness Podcast



## Website

<https://www.dchatte.com/>



## Email

[dchatte@gmail.com](mailto:dchatte@gmail.com)