ALCHEMY CYBER

Decoding Cyber Risk Governance: A Blueprint for Sustainable Business Resilience

Effective Strategies for Board Oversight

Anand Thangaraju, CISSP
Founder & CEO, Alchemy Cyber Inc.

August 2026

About Me

- Cyber Security & Strategy Leader
- Board Advisor & Angel for Startups. Operating/Venture Partner for VCs
- Past Operator at Cognizant, JPMC, EY, SVB, Zelle, ePlus
- Fractional CISO and Strategic Partner (VAR) to CISOs
- Regular Speaker at Conferences (RSA, BlackHat, SINET, HMG, CRA etc.)
- Certified in ORM, CERP, CISA, CISSP, CIPM, SCR and many more

Anand Thangaraju

Founder & CEO,
Alchemy Cyber Inc.

Alchemy Cyber

Introduction

The cyber-threat landscape we face today is more complex and dangerous - cybercrime is expected to cost the world some **$12 trillion dollars** in 2030.

We need **a new model** of sustainable cybersecurity.

With commitment at **the board level.**

Cyber risk is no longer a mere technical concern managed by IT departments - but a critical strategic issue that impacts entire enterprises:

Cyber Risk as a strategic issue in Corporate Governance:

01

Enterprise-Wide Impact:

Can affect a company's reputation, operational continuity, and financial performance.

02

Strategic Value Creation:

Effective cybersecurity can preserve and even create strategic value by protecting the organization's digital assets and fostering trust with customers and stakeholders.

03

Board Oversight:

The board has a role in cyber risk management framework. This can include regular assessment and oversight of how well cyber risks are being identified, managed, and mitigated.

Let us consider a hypothetical scenario imagined at a US pharmaceutical company

A CISO recommends the company fund a **phishing-resistant multifactor authentication (MFA) tool** for all employee accounts. It's a mere 5% spend on his shrinking Annual budget.

Company leadership **declines,** based on their judgment about the likelihood of a cyberattack based on past history.

An attacker tricks a user into revealing their login credentials, **data is exfiltrated and systems are shut down** by ransomware.

Possible Damages

01 **Delayed shipment** of critical pharmaceuticals, resulting in delayed surgeries across the country

02 **Theft of sensitive customer data,** resulting in identity theft and personal financial impact to millions of customers

03 **Theft of critical intellectual property,** eventually sold to an overseas company owned by an adversarial nation, which brings several competing drugs to market years ahead of schedule, with downstream effects on market share

04 Over time, the US healthcare system begins to rely heavily on the overseas company for the pharmaceuticals, which ultimately **damages US competitiveness** and its leverage in the event of a geopolitical conflict

Cyber Threats

by the numbers

1. Global annual losses from cybercrime are estimated to reach **$12 trillion by 2030**.
2. The United States is the costliest place in the world to face a breach.
3. On average, breaches were not detected until 180 days after the breach had occurred. (IBM Report)
4. It typically takes 60 days to contain a breach in 2026.

Data Breach Costs	The global average cost of a data breach fell to **$4.44 million in 2025** — down ~9% from $4.88M the prior year, the first decline in five years, credited to faster AI-powered detection.
Cloud Exploitation	Cloud intrusions surged **136% in the first half of 2025** versus all of 2024, and state-linked "cloud-conscious" intrusions rose 266%. Abuse of valid accounts now drives roughly 35% of cloud incidents
Email as a Primary Entry Point	Email remains the leading way in: roughly **68% of cyberattacks originate from email**, and phishing was the single most common initial access vector in breaches.
Malware-Free Attacks	Identity-based, malware-free techniques now dominate: **82% of detections in 2025 were malware-free** (up from 79% in 2024).
Ransomware Attacks	Ransomware remains widespread, with ~**72% of organizations reporting attack attempts in 2025**. Payment behavior is shifting: IBM found ~63% refused to pay.

The Role of the Board in Cybersecurity

01. Integration into Risk Management

Ensure that cyber risk is integrated into the company's overall enterprise risk management framework. Cyber risk should be treated as an enterprise-wide strategic risk, not just an IT issue.

02. Define Oversight Roles

Clearly define and assign oversight responsibilities, either at the full board level or within designated committees, such as audit or risk committees.

03. Regular and Adaptive Reporting

Management should provide regular and flexible reports to the Board about the company's cybersecurity posture, reflecting the evolving threat environment.

04. Engagement and Healthy Skepticism

The Board should engage with cybersecurity leaders (e.g., the CISO) while maintaining healthy skepticism. Directors should verify all information provided.

05. Independent Assessments

Boards should leverage independent third-party assessments to validate the company's cybersecurity efforts.

06. Education and Continuous Learning

Board members should participate in continuous education on cybersecurity trends and regulatory changes.

Principle 1: Cybersecurity as an Enterprise & Strategic Risk

01 Increasing Financial Impact:
The Change Healthcare ransomware attack cost parent company UnitedHealth Group approximately $3.1 billion in direct breach response costs through 2024 and impacted 60% of US population

02 Regulatory and Legal Exposure:
The largest GDPR fine of 2025 was €530 million against TikTok parent company ByteDance for unlawful international data transfers to China, issued by Ireland's DPC in May 2025

03 Business Disruption and Downtime:
Colonial Pipeline was forced to halt operations in 2021 due to a ransomware attack, causing a nationwide fuel shortage.

04 Reputation and Trust Damage:
Target 2013 breach of 40 million customer credit cards caused significant reputational damage, which impacted its market value

05 Supply Chain Vulnerabilities:
The SolarWinds breach in 2020, which compromised several U.S. federal agencies, highlighted the systemic risk from third-party software.

06 Data as a Core Asset:
Facebook's 2018 Cambridge Analytica scandal demonstrated how mismanagement of data security can have significant strategic consequences.

Key Considerations for the Board

01 Hardwire cyber-risk considerations into key operational and strategic decision-making processes, including the adoption of cyber risk as a recurring agenda item for full-board meetings.

02 View each major new digital transformation initiative through the lens of cyber risk.

03 Analyze cybersecurity issues with respect to their strategic implications and as part of the total enterprise risk exposure.

04 Analyze business strategy and business-model considerations with respect to cybersecurity Issues.

05 Ask executives to identify opportunities to use cybersecurity as a market differentiator and business driver.

Principle 2: Legal and Disclosure Implications

Here are six emerging trends in Global Cybersecurity Regulations:

01 **Increased Cybersecurity Legislation in the U.S.:**
Law makers across 37 US states passed 99 cybersecurity-related bills in 2025, establishing 393 new cybersecurity rules

02 **Revised Regulatory Standards in 2026:**
FTC safeguards Rule - financial institutions must now notify the FTC as soon as possible, and no later than 30 days after discovery, of a security breach

03 **SEC's Proposed Rules for Cybersecurity:**
The U.S. Securities and Exchange Commission (SEC) started enforcing their proposed rules which require detailed information about cybersecurity governance and board oversight since Dec 2023

04 **Critical Infrastructure Act (CIRCIA):**
Critical infrastructure operators will have to notify CISA within 72 hours of discovering a "covered cyber incident" and within 24 hours of making a ransom payment.

05 **European Regulatory Changes:**
The European Union updated regulations like the Network and Information Security Directive (NISD2) and introduced the Digital Operational Resilience Act (DORA), emphasizing incident reporting and oversight of third-party vendors.

06 **Expansion of GDPR-Like Regulations Globally**
Other countries, such as Australia, Brazil, South Africa, and India, have been enacting data protection laws similar to the EU's General Data Protection Regulation (GDPR).

Key Considerations for the Board

Board members should carry out regular sessions on legal, regulatory, or contractual trends and recent developments in cybersecurity.

01 Consider whether any new business endeavors or partnerships generate new and differing legal obligations.

02 Consider whether oversight responsibility for cybersecurity should reside with the full board or with a board committee.

03 Consider whether the board has access to appropriate cyber expertise, either through its own composition or via access to management experts, consultants, and legal advisers, or a combination of these resources and assets.

04 Ensure that management has developed the appropriate level of relationships and line of communications with relevant regulatory and enforcement entities.

05 Ensure that the internal legal team has relationships with outside counsel to aid in special events such as incident response. Define the governance structure for disclosing material risks and actual incidents to regulatory authorities.

06 Periodically review with management the information systems and controls related to cyber risks.

SEC Regulation requirements

Current Incident Reporting

The SEC requires companies to disclose material cybersecurity incidents using SEC Form 8-K within four days of determining the incident's material impact.

Periodic Risk Management Disclosures

Companies must regularly disclose their cybersecurity risk management policies and procedures, detail management's role in these efforts.

Use of InLine XBRL Format:

The SEC mandates that cybersecurity disclosures be presented in InLine eXtensible Business Reporting Language (XBRL) to improve transparency and accessibility for investors, aiding in the analysis of disclosures.

Board's Oversight Role

The SEC emphasizes that companies should clarify how the board engages in cybersecurity oversight. This includes disclosing the frequency of cybersecurity briefings.

Disclosure of Cyber Expertise:

Companies are required to state whether any board members have cybersecurity expertise and describe this expertise in detail, allowing investors to assess the board's ability to manage and oversee cyber risks effectively.

Governance and Internal Controls:

The SEC stresses the importance of implementing and maintaining governance protocols to ensure accurate reporting.

Principle 3: Board Oversight Structure and Access to Expertise

Cyber-Risk Oversight Practices by the Board

Key Considerations for the Board

Establish key cybersecurity structures, committee assignments, and a cadence for review of information, and ensure that cybersecurity oversight is a topic integrated into the onboarding of new directors.

01 Ensure that the board has access to the appropriate expertise from inside and outside the company to help it perform oversight duties with confidence.

02 Establish an organization-wide culture of cybersecurity culture from the boardroom and encourage collaboration across all stakeholders relating to and accountable for cyber risks.

03 Take great care when considering the addition of a cybersecurity expert to the board to ensure that this person doesn't become the sole repository for cyber-risk oversight.

Principle 4: Enterprise Framework for Managing Cyber Risk

Multiple technical frameworks have been developed to act as sets of best cybersecurity practices:

01 The **National Institute of Standards and Technology Cybersecurity Framework** (NIST CSF) - The NIST CSF's risk management process includes five key functions (identify, protect, detect, respond, and recover) and more than one hundred cybersecurity best practice activities.

02 The **International Organization for Standardization (ISO)** created the ISO/IEC 27000 family of standards as a series of best practices to help organizations improve their information security through security controls.

03 The **Center for Internet Security's CIS Critical Security Controls** include a list of 18 security controls with a prioritized set of actions to protect organizations and data from cyberattack vectors.

04 The 15 **PCI Security Standards** by the PCI Security Standards Council are a set of best practices designed to help organizations "protect payment account data throughout the payment lifecycle.

Key Considerations for the Board

Boards should expect management to incorporate cyber risk into an enterprise risk-management approach.

01 In order to provide full oversight of cyber risks, management should adopt both technical and management frameworks.

02 There are several technical and management frameworks that can be adopted and adapted to the unique needs of an organization.

The ISA-ANSI approach

The Internet Security Alliance (ISA) and the American National Standards Institute (ANSI) have developed a multi-stakeholder model outlining the following seven steps:

1. **Establish ownership of cyber risk on an interdepartmental basis.**
2. **Appoint an organization-wide cyber-risk management team.**
3. **The cyber-risk team needs to perform a forward looking, enterprise-wide risk assessment, using a systematic framework.**
4. **Be aware that cybersecurity regulation differs significantly across jurisdictions and from industry to industry A**
5. **Take a collaborative approach to developing reports for the board. Executives should be expected to track and report metrics.**
6. **Develop and adopt an organization-wide cyber-risk management plan and internal communications strategy across all departments and business units.**
7. **Develop and adopt a comprehensive cyber-risk budget with sufficient resources to meet the organization's needs and risk appetite.**

Principle 5: Cybersecurity Measurement and Reporting

How are we measuring the threat environment and how prepared are we to meet it?	• Global cyber-related financial and data losses • Threats and new breaches within our industry that are most likely to introduce business, operational, and financial harm into our organization • Trends in the types of hacker tactics (e.g.,ransomware, leveraging zero-day vulnerabilities, etc.) and new attack patterns • Cyber threat trends from information sharing and analysis centers (ISACs)
What is our cyber-risk profile?	• Independent security assessments (e.g., external consultants, law firms specializing in cybersecurity and privacy laws, and auditors) • Independent security ratings of the company, benchmarked against peer organizations and used alongside other key risk indicators to augment understanding • Third-party and fourth-party risk indicators
What is our cyber-risk profile as defined by management?	• A NIST-based program maturity assessment conducted by a third party • The relationship between cyber-risk maturity and risk-mitigation prioritization • Investments made to ensure business resilience • Compliance metrics on basic cyber hygiene (the Five Ps): Passwords, Privileged Access, Patching, Phishing, and Penetration Testing • Percentage of critical systems downtime, and time needed to recover • Mean time to detect and remediate cyber breaches
What is our cyber-risk exposure in economic terms?	• Value of enterprise digital assets, especially the company's crown jewels • Probability of cyber event occurrence and potential loss magnitude • Potential reputational damage and impact on shareholder value • Costs of developing and maintaining the cybersecurity program • Costs of compliance with regulatory requirements (e.g., the EU's General Data Protection Regulation)

Cyber-Risk Quantification Approaches and Method

This can lead to two types of effects:

01 Asset-Based CRQ

These models mostly perform risk analysis via an asset register alongside a risk register to then quantify a company's cyber-risk exposure in economic terms.

While robust at the asset level, these models do not always evaluate risk to the organization and ecosystem.

02 Actuarial-Based CRQ

This approach leverages historical actuarial data related to breach and loss events to calculate cyber-risk exposure, potential loss magnitude, and likelihood of risk event.

Cyber insurance actuarial data in this space is highly variable. Additionally, this model is unable to account for zero-day attacks and newly discovered vulnerabilities as, by definition, they lack historical actuarial data on those methods of attack.

Questions directors can ask to better understand their organization's chosen approach:

- Does the chosen CRQ model have any weaknesses? How is the cyber-risk management team mitigating what the model doesn't cover?
- Is the chosen model flexible enough that we are regularly updating it to address new vulnerabilities and recent cybersecurity events?
- Is the approach we are using in line with those of our sector and industry peers?

Principle 6: Systemic Resilience and Collaboration

01 Fostering Systemic Resilience:
Consider cybersecurity as an interconnected challenge. Boards should promote systemic resilience through proactive collaboration with public and private stakeholders

02 Collaborative Cyber Defense:
Boards are encouraged to work together across industries to establish collective defenses.

03 Ecosystem-Wide Responsibility:
Champion a collective responsibility mindset, where cyber resilience is treated as a shared duty.

04 Awareness of Interdependencies:
Boards should understand how their organization's cybersecurity practices impact and are influenced by the broader digital ecosystem. The principle highlights examples such as the **NotPetya** and **SolarWinds** incidents to illustrate the interconnected nature of modern cyber threats.

Key Considerations for the Board

Develop a **360-degree view** of the organization's risk and resiliency posture to function as a socially responsible party in the broader environment in which the business operates.

01 Develop peer networks that include other board members to share best governance practices across institutional boundaries.

02 Ensure that management has plans for effective collaboration and information sharing, especially with the public sector, on improving security and resilience.

03 Ensure that management takes into account risk stemming from broader industry considerations (e.g., third-party vendors and partners.

04 Encourage management's participation in industry groups and knowledge and information sharing platforms such as sector-specific information sharing and analysis centers (ISACs) and/or cross-sectoral information sharing organizations (ISOs).

Ransomware Readiness

Readiness

1. Is there a playbook for ransomware and expected outcomes?

2. What are our cyber capabilities and/or countermeasures?

3. What percentage of coverage do these capabilities provide across our digital/IT estate?

Response Exercises

1. Is there a clearly communicated line of accountability in the event of an attack?

2. Are there clear thresholds related to the materiality of an attack, including triggers for engagement of the board?

3. Are we ready to coordinate with law enforcement in the event of a ransomware attack?

Backup and Recovery

1. How are our system backups maintained, tested, and measured for resiliency?

2. In the event of a ransomware attack, are we confident that our IT systems can be restored within our specified recovery plan objectives?

3. Do our system' response times align with our current timelines in recovery plan?

Communications

1. Is there a concise communications plan across cybersecurity and technology teams and senior management?

2. Does the plan include holding statements for various audiences (e.g., employees, customers, regulators, media)?

Suppliers and Partners

1. Do we monitor critical third parties for ransomware attacks?

2. Do we require specific ransomware and/or incident reporting from third parties within our ontracts and agreements?

3. Do we assess (and reassess incrementally) any third parties to understand their cyber-risk posture?

The Cyber-Insider Threat

Insider threat can be defined as the potential for an individual or individuals with authorized access or understanding of an organization to harm that organization. This risk will be more prominent in the agentic world.

Questions Board should ask:

1. **What is our probable loss exposure related to the insider threat scenarios?**
2. **How does the organization measure the effectiveness of its insider threat mitigation plan?**
3. **Does the organization have a documented insider threat mitigation plan with clearly designated oversight, management, and reporting responsibilities?**
4. **What manual and automated systems are in place to vet employees and identify anomalous behavior throughout the employee life cycle?**
5. **How are third-party vendors monitored to control unauthorized access?**
6. **Does the organization have adequate programs in place to sensitize employees to insider risks and train them?**

Supply Chain and Third-Party Risk

The strength of an organization's cybersecurity can be undermined by the weakest link in its supply chain.

On cost and dwell time, a supply chain compromise now costs $4.91 million on average and takes 267 days to identify and contain, the longest lifecycle of any breach vector tracked by the IBM 2025 report, and supply-chain breaches cost roughly 17x more to remediate than direct, first-party breaches.

For instance, attackers in the high-profile **2021 SolarWinds breach.**

Successfully competing in the digital age may require using a long and global supply chain, including the use of third-party technologies and software.

Questions Board should ask:

1. How do we balance the financial opportunities with potentially higher cyber risks?
2. How much visibility do we have across our supply chain regarding cyber-risk exposure?
3. How to fully include cybersecurity in current supply-chain and vendor/third-party risk management?
4. How difficult/costly will it be to enhance monitoring of access points in the supplier network?
5. Do our vendor agreements bring new legal risks or generate additional compliance requirements?

Case Study 1: Failure in M&A Due Diligence

Unidentified Risk During Acquisition Due-Diligence Led Marriott Directors to Face Violation of Security Law Claims and Personal Liability Lawsuits

1. In August 2018, **Marriott International** acquired Starwood Hotels and Resorts Worldwide for **$13 billion.**
2. However, Marriott's board failed to identify a data breach in the Starwood guest reservation database from 2014, **resulting in the loss of sensitive data for more than 380 million people.**
3. Sensitive data included **names, payment card data, passport information, travel companions, and home addresses.**
4. Even though the breach occurred two years prior to the acquisition, **Marriott learned about the breach in September 2018,** one month post acquisition.
5. Investigations were opened. Marriott directors were personally named in US court filings, and they defended their oversight in court.

These lawsuits, fines, and consequent reputational damage could have potentially been avoided or more effectively managed if Marriott had identified this data breach

Case Study 2: Investors Sue SolarWinds Directors Claiming Failure to Monitor Known Cyber Risks

1

In the spring of 2020, **SolarWinds** sent out an update to its network-monitoring Orion software.

2

However, **malicious code was embedded** into the update, creating backdoor access to customer systems. An estimated **18,000 businesses** were affected, and impacted even government agencies.

3

In November 2021, pension funds and individual shareholders **filed a lawsuit** claiming current and former board directors breached their fiduciary duty of care.

4

In October 2022, SolarWinds settled in court to **pay shareholders $26 million,** alleging violations of US federal security laws with respect to cybersecurity disclosures and public statements.

Director knowledge of cybersecurity and frequent reviews of cybersecurity risks and associated policies, processes, and controls proves to be key in providing adequate oversight.

Case Study 3: Ransomware Attack on Critical Infrastructure

Ransomware Attack Disrupts Global Supply Chains!!

1. Despite being warned by researchers of their software vulnerabilities, **in 2021** a **Kaseya** suffered a ransomware attack on its virtual system administrator software.
2. The **company's software was used by large IT companies** that offered services to hundreds of small and medium sized businesses (SMBs).
3. As a result, the **company told nearly 40,000 customers** to disconnect their services.
4. Nearly **1,500 businesses**—predominately SMBs—had their operations disrupted worldwide.

Arguably the largest ransomware attack yet—was successful in disrupting global supply chains over the long Independence Day weekend.

Key Takeaways: Cyber Security and the Board

Embed Cyber Risk into Strategic Oversight:

Make cybersecurity a central topic in strategic and risk management discussions, ensuring it’s a standing agenda item in board meetings.

Strengthen Board Expertise:

Invest in continuous education and training for board members on emerging cyber threats and regulatory changes, and engage cybersecurity experts as needed.

Scenario Planning and Preparedness:

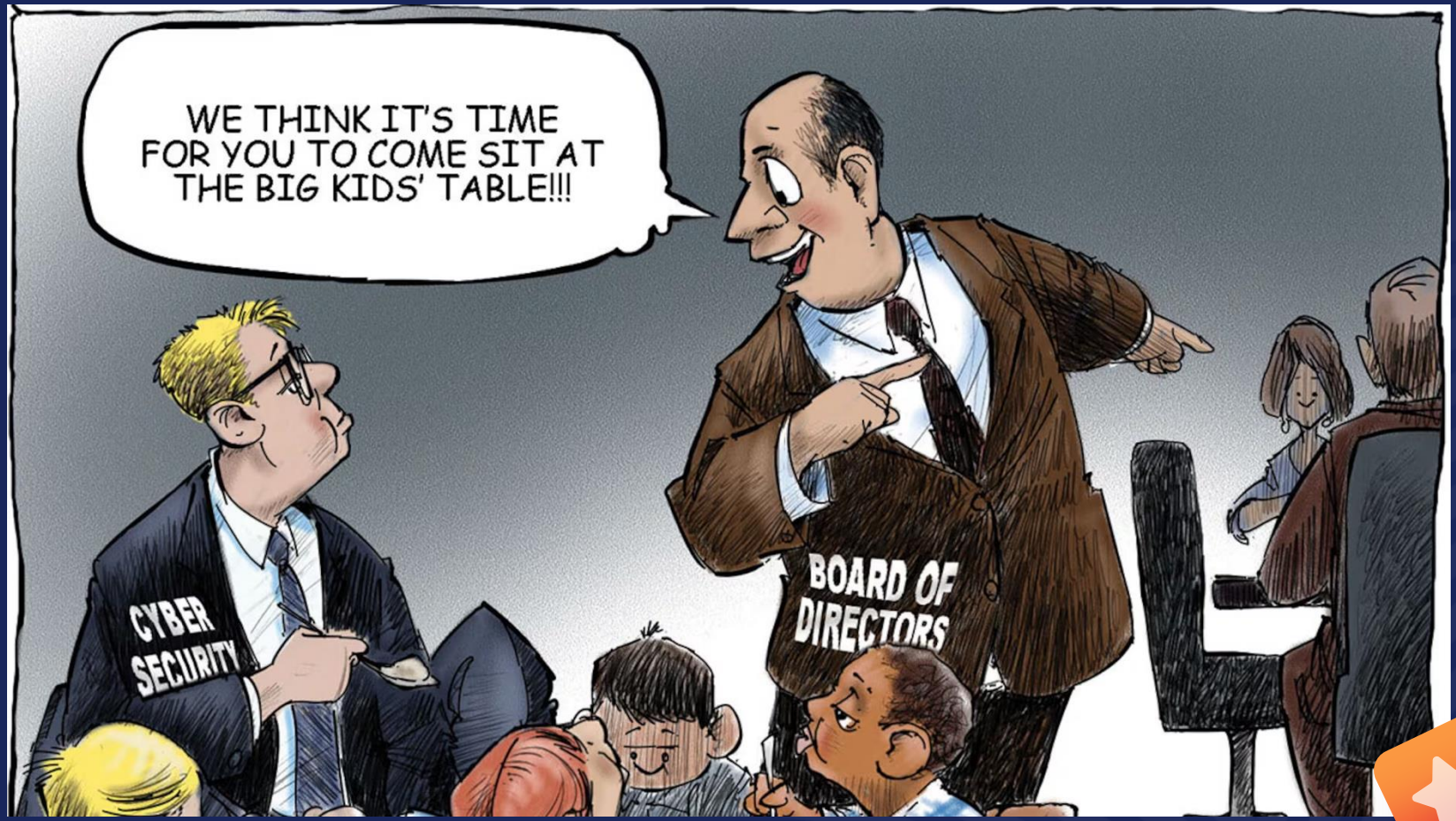
Participate in cyber incident response simulations and tabletop exercises to ensure that the board and management are well-prepared for potential breaches.

Promote Collaborative Cyber Defense:

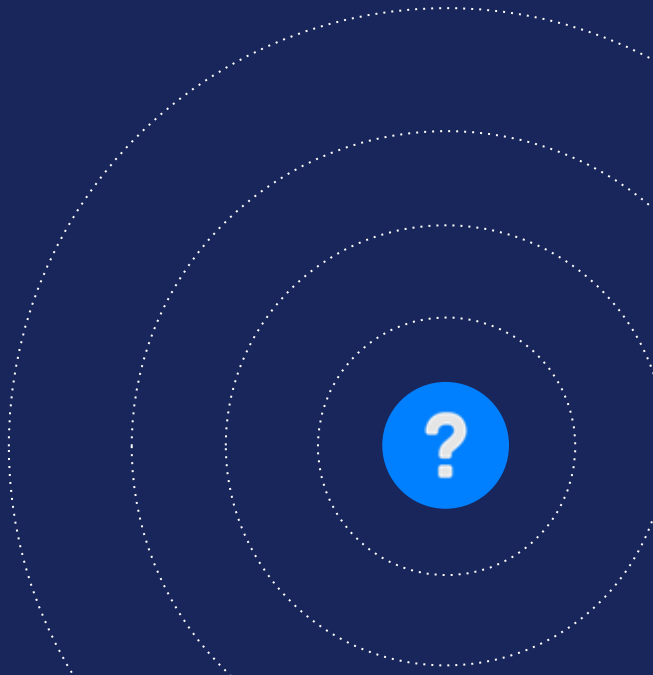
Advocate for cross-industry collaboration and partnerships with governmental agencies to strengthen collective cyber resilience.

Regularly Review and Audit Cybersecurity Programs:

Use independent third-party assessments to evaluate the effectiveness of the organization’s cybersecurity framework and ensure continuous improvement.


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS

Questions ?



Reporting Incidents to FBI

What the FBI does in response to a reported cyber incident:

Identify and stop the activity.

- Information sharing
- International partnerships:
- Recovery Asset Team (RAT):
- Apprehend or impose costs on cyber actors

Seize or disrupt the actor's technical infrastructure

Share valuable insights from other investigations that may help.

Support your organization's data-breach response.

What Should be Reported?

Technical data and incident information can prove helpful for investigators:

1. Indicators of compromise (IOCs), ie. threat actor IP addresses.
2. Threat actor tactics, techniques and procedures (TTPs)
3. Threat actor communications - ransom notes, TOR addresses
4. A timeline of the event
5. The nature of the incident
6. A point of contact for regular communication with investigators
7. Logs from the affected machines
8. Images of the affected machines
9. Actions that have been taken
10. Forensic reports from any incident response firm that has been contracted

How to Contact the FBI?

- Local FBI Field Office: https://www.fbi.gov/contact-us/field-offices
- The FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/
- Online Tips and Public Leads Form: https://tips.fbi.gov/
- FBI Tip Line: 1-800-CALL-FBI (1-800-225-5324)
- International FBI offices: https://www.fbi.gov/contact-us/legal-attache-offices
- National Cyber Investigative Joint Task Force https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force)
- NCIJTF CyWatch 24/7 Cyber Center:
  To contact CyWatch, please call 1-855-292-3937 or email cywatch@ic.fbi.gov

Thank you

Anand Thangaraju

CISO, Board Director, Investor, Product GTM,
VC Catalyst, Mentor, Speaker