CYBERSECURITY & INCIDENT MANAGEMENT
A GOVERNANCE IMPERATIVE FOR FINANCIAL STABILITY

May 5, 2025

Amy Mushahwar

Chair, Privacy & Data Security

TRUE CYBER RESILIENCE STARTS WITH MANAGEMENT

WE NEED A NEW MODEL OF SUSTAINABLE CYBERSECURITY. ONE THAT STARTS WITH A COMMITMENT AT THE BOARD LEVEL TO INCENTIVIZE A CULTURE OF CORPORATE CYBER RESPONSIBILITY IN WHICH MANAGING CYBER RISK IS TREATED AS A FUNDAMENTAL MATTER OF GOOD GOVERNANCE AND GOOD CORPORATE CITIZENSHIP.

Jen Easterly, Former Director of CISA

**Sean Plankey's nomination is on hold pending a request of Senator Wyden re Salt Typhoon impacting the telecom industry.*

ENERGY SECTOR FACES MANY OF THE SAME THREATS AS GENERAL PRIVATE INDUSTRY

Traditional vendors as well as "table stakes" technology (software, SaaS, VPNs, monitoring, MSSPs)

Gone is the Lone Wolf: Attacker Professionalization / Specialization

- Access Brokers
- Exploit
- Negotiation

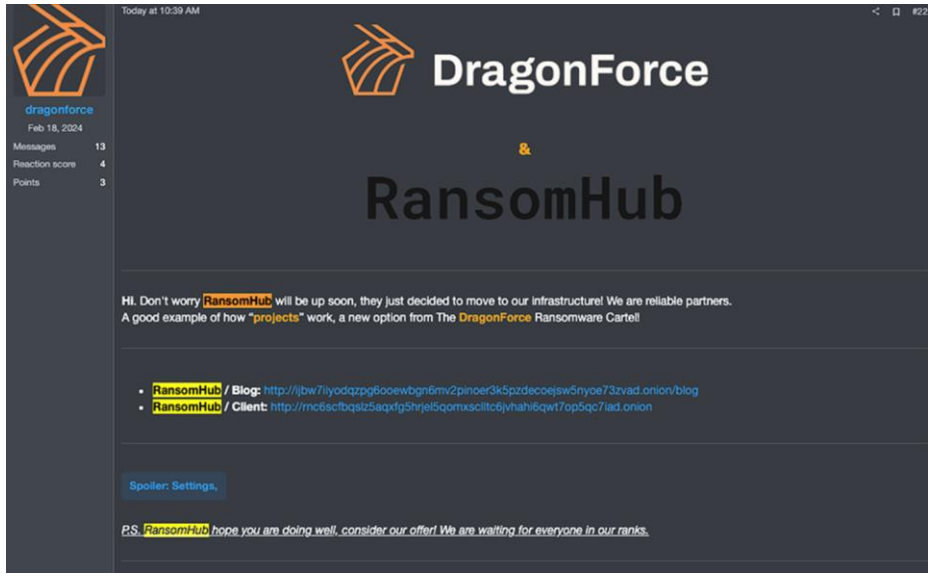
Other breach headwinds: M&A activity, lack of a fully mapped data and operational environment, legacy technology, retail environments, IP/PII

ENERGY SECTOR IS IN THE CROSSHAIRS

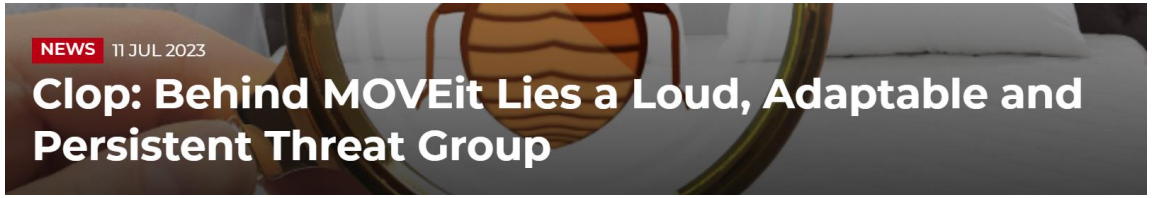
Digital Transformation - Cloud Adoption, Automation

Operational Technology

Geopolitical Concerns / Hacktivism



Haliburton's RN: 35M in losses (est.)



15 Companies in the Energy Sector Compromised by Cl0p – MOVEIt

CISA CUTS/ADMINISTRATION STAFFING SHIFTS IN CYBER DEMAND COMPANIES PROTECT THEMSELVES

GOVERNMENT

Trump administration proposes cutting $491M from CISA budget

A budget summary doesn't give specific details on which programs it would cut, instead providing a broad outline.

BY TIM STARKS • MAY 2, 2025

NATIONAL SECURITY

McCabe suggests FBI 'spreading their terrorism resources too thin' with recent immigration activity

BY FILIP TIMOTIJA - 03/25/25 3:49 PM ET

AWAITING FINAL RULE ON CIRCIA FOR 72H BREACH AND 24H RANSOM PAYMENT NOTICE

Note: The Final Rule on notification under CIRCIA has NOT been published, once published, the Rule would have 18 months to take effect.

However, elements of reporting occur regardless as apart of the government contract process and FINCEN-SAR.

LITTLE PII? BREACHES MATTER WITH B2B.
CYBER LEGAL OBLIGATIONS WITH B2B CLIENTELE

We are aware of the legal obligations for PII (both consumer and employee). The risk can be greater with B2B clientele – usually many more entities capable of suing you, and ordinarily there are 24-, 48- and 72-hour notification obligations.

- **Critical Infrastructure**
- **Government Contracts**
- **State laws** regarding cybersecurity (e.g., state reasonable security laws and general negligence statutes)
- **State data breach laws** that are not limited to individual PII (some states include corporate information)
- **Contractual obligations –** for all
- **Main driver** – potential loss of customers, especially during a rough operational year

IN B2B FINANCE: WHY DO I CARE?

Breaches Impact Cash Flow

Many expenses, not all insurable

Companies cannot always book revenue

TABLE OF CONTENTS

1. What Is the Role of Management in Cyber Governance?
2. What Questions Should Management Ask to Manage Company Cybersecurity Risk?
3. What is Senior Management's Role in a Cyber Incident?
4. Operational Technology Security Still Emerging
5. Industry Trends for Management
6. NYDFS/NYCRR 500 What is New with the Finalization of the 2nd Amendment

ROLE OF MANAGEMENT IN CYBERSECURITY GOVERNANCE

Ensure that legal/security cyber requirements are known and managed.

Determine risk management appetites and ensure there are clear lines of communication to escalate risk.

Allow for strategic initiatives to be included in organizational cyber risk decisions.

Policies are established (by operational teams) but approved and enforced by management.

CISOs are empowered with the influence and resources to address risk.

Direct management to ask about the security of vendor supply chains and ensures that KYC controls are robust.

Ensure management is aware of and assists in the management of cyber incidents.

- For reference, see: NIST Cybersecurity Framework (Govern Controls), available at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf and;
- NACD Director's Handbook on Cyber-Risk Oversight, available at: https://www.nacdonline.org/all-governance/governance-resources/governance-research/director-handbooks/nacd-directors-handbook-on-cyber-risk-oversight/

LINES OF CYBER DEFENSE TO HELP INFORM THE MANAGEMENT TEAM

- **Line 1:** Operational Risk – IT implementors and at Headquarters
- **Line 2:** CISO / Cyber Risk Team
- **Line 2.5:** Legal (not a true line check: it's a consultation role with Lines 1 & 2 as well as Management)
- **Line 3:** Internal and External Audit

Your role – Cyber Success Enabler in Chief.

- *Constantly ask whether your lines of defense have the resources to do their jobs effectively*
- *If not, what can/should you prioritize understanding that resources are finite*
- Request artifacts of security compliance
- *Ask difficult questions of IT and ISO Teams*
- *Hold them accountable*

WHAT IS SENIOR MANAGEMENT'S ROLE IN THE CYBERSECURITY PROGRAM

1. **Set the tone and vision** of the cybersecurity program by establishing a culture of security emphasizing its importance and integrating it into the organization's core values and mission.

2. **Provide strategic oversight** by developing and endorsing cybersecurity strategy and ensuring alignment with business objectives.

3. **Resource allocation**: Appropriating adequate budget and resources to cybersecurity initiatives for technology, personnel and training.

4. **Policy and Governance**: Approving and enforcing cybersecurity policies and procedures to ensure comprehensive protection and compliance.

WHAT IS SENIOR MANAGEMENT'S ROLE IN CYBER PROGRAM (*CONT.*)

5. **Risk Management**: Identify, evaluate, and prioritize cybersecurity risks and ensure appropriate risk management strategies are in place.

6. **Incident Management**: Oversee development and implementation of incident response plans.

7. **Performance Monitoring**: Review regular reports on cybersecurity performance and metrics to assess effectiveness and make informed decisions.

WHAT QUESTIONS SHOULD BE ASKED TO HAVE EFFECTIVE CYBERSECURITY

WHAT QUESTIONS SHOULD BE ASKED TO MANAGE CYBERSECURITY

1. **What is our current cybersecurity posture; what are our strengths and vulnerabilities?**
   - Are there any high-risk concerns that need to be funded (or have not been funded)?
   - What evidence do we have to back up our current security posture?
   - Are there any evidentiary concerns, if a regulator or partner asked us to demonstrate compliance?

2. **What are our critical assets, dependent operational technology and data, how are we protecting them? Do we have those assets mapped (and where do they sit)?**

WHAT QUESTIONS SHOULD BE ASKED TO MANAGE CYBERSECURITY (*CONT.*)

3. **What departments does security collaborate with to ensure it is aware of business line cyber risks?**
   - Do we have mapped out what functions are performed by:
     - Offices
     - Vendors
     - Headquarters

4. **How are we managing dependency risk?**

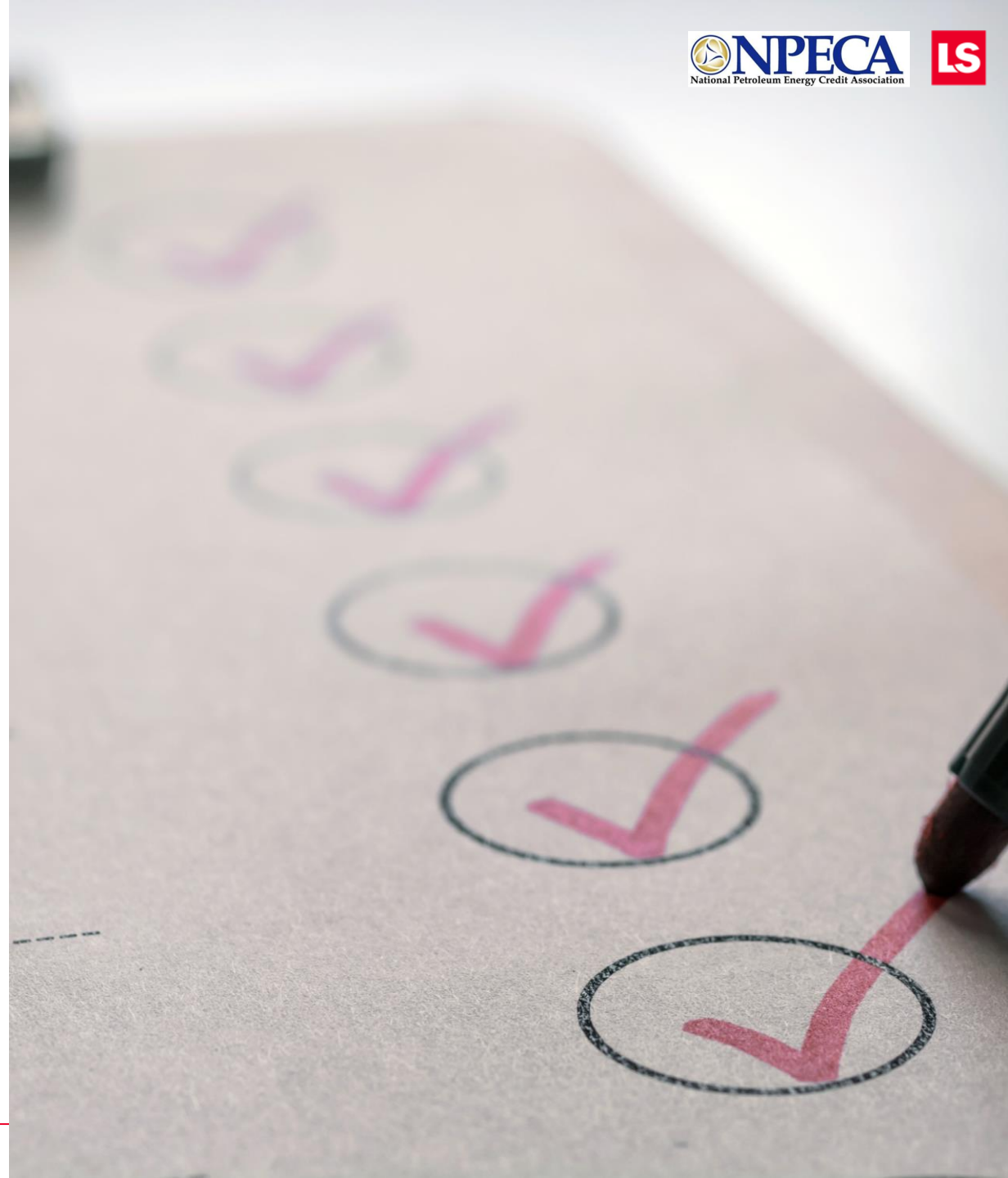
5. **What are the risks and threats to our business and how are we managing them?**

EXAMPLE OF GENERAL RISKS AND HOW THEY ARE MANAGED

Industry Attack	Our Mitigations	Mitigation Enhancement Needed?
BOT Attacks: globally distributed indiscriminate attacks to harvest data from accounts / APIs / or steal funds from account interfaces / encrypt – lockup systems	Web Application Security Firewall (WAF) End-Point Detection Software Next Generation Firewalls	Consider web proxy (Cloudflare) Conduct external scans of true perimeter for insecure protocols (e.g. RDP/Telnet) Consider enhancing patching and SDLC programs to strengthen vulnerability management.
Phishing / Smishing	Email security gateway + employee training and awareness program	
Data Loss Prevention (from inadvertent and malicious disclosure)	Data loss prevention tools + employee training and awareness	Consider a malicious insider program

KNOW A FEW KEY DETAILS FROM YOUR IT HEAD AND CISO

1. Are we implementing Multi-Factor Authentication (“MFA”) appropriately?
2. Do we have endpoint detection and response software?
3. What is the status of our backups as well as business continuity and disaster recovery plans? May I see this documentation and the business impact analysis?
4. Do we have an asset inventory?
5. Do we inventory who our vendors are and what data they have?
6. Do we prioritize secure configurations (for computing assets as well as software and cloud resources)?
7. Do we have any key vendors in security remediation status?
8. What are you most worried about?



WHAT IS SENIOR MANAGEMENT'S ROLE IN A CYBER INCIDENT

IMMEDIATE RESPONSE

Breaches demand operational excellence and effective crisis management

- **Outage Issue or Other Material Impact to Business?**
  - Ask what this is repeatedly, impact will change
  - Any connections that must be immediately severed?
  - Most costly portion of the process
  - Often immediate, so central outage issues must be pre-planned and workshopped
  - Government contract impact?
- **Material Impact for Purposes of the SEC?**
- **Scale Crisis Response and Third-Party Management?**
  - Now often thousands of entities
  - Know your 'whales' for each business line of impact
- **Artifacts Requested by Third Parties**
  - Description of the Incident
  - Remediation Statement
  - SIG/Vendor Security Attestation
  - With Downstream Consumers – What PII obligations will you as the vendor undertake (individual, regulator notifications?)?
  - Customer Calls – Can you scale technical to technical calls?

COMMUNICATIONS CASCADE

TOP 20

- Receive a Phone Call
- Communications packet sent by us
- Should we drive to Third Party call center or one of you?
NoPII

ACTIVE CLIENTS

- Mass email from vendor
- Follow-up call center manned by vendor
- No PII

EMPLOYEES

- Bulk email
- Credit Monitoring
- Early Next Week
- Separate call center for Employees

DEPENDENCIES

- Working website breach page
- All call centers w/ messaging
- Data

POST-INCIDENT RESPONSE MANAGEMENT AFTER ACTION QUESTIONS

What key questions should management ask to avoid repeating a similar attack:

- **Post Incident Review and Establish Root Cause Analysis:** May I review the incident report or related summary? So, I know what happened and what security controls must be enhanced.
- **Validation / Follow-up:** Ask if all incident response provider recommendations were followed and validated, if necessary.
- **Self Examination:** Are there any necessary security or incident response policy changes that we must do to remediate from the incident? (Did our process work smoothly? What could be done better?)
- **Third-Party Vendor Review:** If a vendor incident occurs, have we asked the vendor to validate security and provide an incident summary? Is the vendor fully cooperating with us on all regulatory requests? Going forward, do I need additional metrics, contractual changes or documentation from the vendor?
- **Training Review:** Do we have any employee training that must result from this incident?
- **Communication Review:** How were our communications with external parties, do we need to document any additional incident operational procedures to capture lessons?

INDUSTRY TRENDS FOR MANAGEMENT

INDUSTRY TRENDS FOR MANAGEMENT

1. **Ransomware Defense**: Enhanced focus and preparation for ransomware attacks, including backup, network segmentation and advanced endpoint strategies.

2. **Third-Party Risk Management**: Strengthening controls and monitoring of third-party vendors and service providers to mitigate risks associated with supply chain attacks.

3. **Incident Response Planning**: Updating and regular testing of the Incident Response Plan to be prepared for cyber incidents.

4. **Emerging Technologies**: What are the security implications of emerging technologies such as AI, quantum computing, blockchain? How do we understand their potential impact on the energy industry?

INDUSTRY TRENDS FOR MANAGEMENT(CONT.)

5. **Increased Regulatory Trends**: Stricter compliance, escalated timetables for reporting and regulatory standards are emerging. These include increased privacy regulations, NYDFS and NY Shield Law.

6. **Greater adoption of advanced threat detection and response**: AI and machine learning technologies for real-time threat detection at the endpoint, network and segment levels (XDR). This enables better automated response and threat intelligence to better identify and mitigate advanced persistent threats.

7. **Implementation of Zero Trust Architecture**: This assumes internal threats are possible and requires continuous verification of user ID and device security. Ask about third-party trust relationships within your enterprise, to determine if they exist.

INDUSTRY TRENDS FOR MANAGEMENT(CONT.)

8. Cyber Insurance: What is needed, why do we need it, what are the benefits.

Do we need it? If capitalized by parent company it is not necessary, if not may need if not independently capitalized.

What is needed? Amount of coverage less important than preparedness. Pre-selected and pre-vetted vendor list with appropriate contracts in place.

Why is it needed? Can be used to prepare for a variety of incidents that include targeted attacks, nation state attacks, as well as opportunistic attacks.

What are the benefits? Minimal as a cost savings device

Why Self Insure? Select your own vendors, avoid US govt subpoenas, avoid providing insurers with forensic report. Avoid premium payments.

NYDFS/NYCRR 500: 2ND AMENDMENT UPDATES

NYDFS/NYCRR 500: 2ND AMENDMENT TIMELINE

Start

December 1, 2023:

500.17: Notification obligations to NYDFS.

April 15, 2024

500.17(b): Certification requirements.

April 29, 2024

500.9: Risk assessments requirements;

500.3: Cybersecurity policy requirements;

500.5(a)(1), (b), and (c): Penetration testing and monitoring requirements and

500.14(a)(3): Training requirements

November 1, 2024

500.4: CISO, management, and board governance requirements;

500.15: Encryption requirements; and

500.16: Incident response and business continuity planning and testing requirements.

May 1, 2025

500.5(a)(2): Scanning requirements;

500.7: Access privilege and password requirements;

500.14(a)(2): Requirements for protection against malicious code;

500.7: For Class A companies, requirements relating to privileged access management solutions and blocking of commonly used passwords and

500.14(a)(2) and (b): For Class A companies, requirements for endpoint detection and response solutions and centralized logging.

November 1, 2025

500.12: MFA requirements

500.13(a): Asset inventory requirements

End

NYDFS/NYCRR 500: 6 CATEGORIES OF CHANGE

1. New Obligations for Larger ("Class A") Companies

- **Independent Audits**: design and conduct independent audits of their cybersecurity programs, using internal or external auditors who are free to make decisions not influenced by the covered entity, at a frequency determined by their individual risk assessment
- **Access Privileges and Management Monitoring**: monitor privileged-access activity, implement a privileged access management solution, and implement an automated method of blocking commonly used passwords
- **Monitoring**: Implement an endpoint detection and response solution to monitor anomalous activity, including lateral movement, and a solution that centralizes logging and security event alerting.

2. New Governance Requirements for CISOs, Management, and the Board

- Additional Board Reporting:
- Board Oversight:
- CEO/CISO Annual Certification
- Material Compliance for Previous Calendar Year
- Acknowledgement of Noncompliance
- Tabletop Exercises and Other Testing
- Annual Risk Assessments

NYDFS/NYCRR 500: 6 CATEGORIES OF CHANGE

3. Additional Technical Requirements

- Multi-Factor Authentication ("MFA")
- Monitoring
- Encryption
- Vulnerability Management
- Asset Inventory
- Access Privileges
- Password Management

4. Business Continuity

- Incident Response Plans
- BCDR Plans

5. Breach Notification Obligations: Expanded to include

- Ransomware Notification Requirements:
- Information Updates

6. Enforcement

- The commission of a single act prohibited by Part 500, or the failure to satisfy an obligation, constitutes a violation.
- The Consideration of Mitigating factors: Cooperation, good faith, intentionality, history of prior violations, harm to customers, gravity of violation, number of violations, involvement of senior management, penalties imposed by other regulators, and the financial resources of the covered entity and its affiliates.

Lowenstein Sandler

NPECA
National Petroleum Energy Credit Association

QUESTIONS?

THANK YOU

NEW YORK
1251 AVENUE
OF THE AMERICAS
NEW YORK, NY 10020
212.262.6700

PALO ALTO
390 LYTTON AVENUE
PALO ALTO, CA 94301
650.433.5800

NEW JERSEY
ONE LOWENSTEIN DRIVE
ROSELAND, NJ 07068
973.597.2500

UTAH
500 NORTH MARKETPLACE
CENTERVILLE, UT 84014
650.433.5630

WASHINGTON, D.C.
2200 PENNSYLVANIA AVE NW
WASHINGTON, D.C. 20037
202.753.3800

lowenstein.com