TAMPER-PROOF EVIDENCE PRESERVATION FOR BOD MEMBERS

SEC CYBERSECURITY REQUIREMENTS FOR CYBER-INCIDENT REPORTING DEMAND THE PRESERVATION OF EVIDENCE FOR PROACTIVE CYBERSECURITY CONTROLS

UNDERSTANDING THE RISK

- The newly proposed SEC cybersecurity incident reporting rules are now available for review requiring the reporting of material cyber-incidents with 96 hours of confirmation
- Require current **reporting about material cybersecurity incidents within 4 days** on Form 8-K;
- Require **periodic disclosures regarding**, among other things:
  - **A registrant's policies and procedures to identify and manage cybersecurity risks;**
  - **Management's role in implementing cybersecurity policies and procedures;**
  - **Board of directors' cybersecurity expertise, if any, and its oversight of cybersecurity risk**; and
  - Updates about previously reported material cybersecurity incidents; and
- Require the cybersecurity disclosures to be presented in Inline eXtensible Business Reporting Language (Inline XBRL).
- The proposed amendments are designed to **better inform investors about a registrant's risk management, strategy, and governance** and to provide timely notification of material cybersecurity incidents.

SEC EXPECTATIONS ON MANAGEMENT ARE CLEAR

- Describe its policies and procedures, if any, for **the identification and management of risks from cybersecurity threats, including whether the registrant considers cybersecurity as part of its business strategy, financial planning, and capital allocation**; and
- Require **disclosure about the board's oversight of cybersecurity risk and management's role and expertise in assessing and managing cybersecurity risk and implementing the registrant's cybersecurity policies, procedures, and strategies.**
- Amend Item 407 of Regulation S-K and Form 20-F to **require disclosure regarding board member cybersecurity expertise. Proposed Item 407(j) would require disclosure in annual reports and certain proxy filings if any member of the registrant's board of directors has expertise in cybersecurity, including the name(s) of any such director(s) and any detail necessary to fully describe the nature of the expertise.**

MANAGEMENT IS RESPONSIBLE FOR CYBERSECURITY

- A failure to properly manage and mitigate cyber-risks could be evidence of negligence with regard to “duty of care” requirements to protect a business
- Directors and Officers could be held personally liable in a shareholder lawsuit resulting from a cyber-incident that results in shareholder losses
- Managers and Officers need to ensure that cybersecurity controls are in place and functioning properly for both PROACTIVE prevention of harm, and REACTIVE detection and remediation/recover from a cyber-incident
- Tamper-proof evidence of these controls will be vital in any shareholder lawsuits aiming to hold officers with fiduciary duties personally liable

WHY NOW

- SEC rules require visibility into cyber-incidents with 96 hours of a material cyber-incident exposing BoD Members and C-Suite Executives to potential lawsuits from shareholders
- Well defined software supply chain controls are broadly available to proactively detect software risk and prevent harm
- Failure to perform proactive software supply chain risk management may be considered negligent behavior with regard to duty of care fiduciary duties

HOW TO PROTECT YOURSELF FROM SOFTWARE RISKS AND LIABILITY

- Implement PROACTIVE software supply chain risk management controls using SBOM's
- Perform a software supply chain risk assessment following best practices provided by NIST (SP 800-161) using SAG-PM ™
- Work with software suppliers to provide a Vendor Response Form (VRF) identifying product SBOM's and an online living NIST SBOM Vulnerability Disclosure Report (VDR) for each software product and version they provide
- Preserve tamper-proof evidence showing that these controls are functioning properly and store this evidence ins a secure evidence locker, such as SAG-CTR ™
- Rely on REA to produce SAG-CTR tamper-proof evidence in court on behalf of the defense (Officers and Directors), in the event of any shareholder lawsuits
- Never trust software, always verify and report! ™

HOW DOES THIS WORK

Software Supplier provides SBOM and other Supply Chain Artifacts (VRF)

Software Consumer performs a NIST C-SCRM compliant SAG-PM Risk Assessment using supplied materials producing evidence data

Evidence data produced by SAG-PM is submitted to SAG-CTR to be stored in tamper-proof format

SAG-CTR ™

Tamperproof Evidence Data is Produced

SAG-CTR Evidence Locker

Tamperproof evidence stored in evidence locker is presented in court when needed

NEXT STEPS

- Contact REA to get started by implementing REA's patented PROACTIVE "Left of Bang" Software Supply Chain Risk Management (C-SCRM) Cybersecurity Controls (SAG-PM ™) for the software supply chain and preserve the tamper-proof evidence in a secure evidence locker (SAG-CTR ™) that may be presented as evidence to prevent personal financial losses in the event of a cyber-incident that results in shareholder lawsuits claiming negligence in "duty of care" responsibilities