CIMCOR

REPORT

Navigating the SEC Cybersecurity Disclosure Rules

Understand, Prepare, and Comply with the New Regulations

TABLE OF CONTENTS

CIMCOR

PART 1

Understand, prepare & comply with the new regulations

In an increasingly digitized world, where businesses rely heavily on technology and data to function, the importance of robust cybersecurity measures cannot be overstated.

Recognizing the growing significance of cybersecurity risk in public companies, the US Securities and Exchange Commission (SEC) has taken a significant step forward by adopting new rules and regulations pertaining to cybersecurity risk management and incident disclosure of public companies. These regulations aim to safeguard investors, promote transparency, and embrace a crucial step in developing cybersecurity governance.

UNDERSTANDING THE NEW RULES AND REGULATIONS

The SEC's new rules and regulations address two main aspects: cybersecurity risk management and incident disclosure.

CYBERSECURITY RISK MANAGEMENT

The regulations emphasize the need for effective cybersecurity risk management strategies within publicly traded organizations. This involves the establishment of comprehensive cybersecurity policies and procedures designed to identify, protect, detect, respond, and recover from potential threats. By implementing these measures, companies can proactively safeguard sensitive data, mitigate cybersecurity risk, and maintain the trust of investors.

INCIDENT DISCLOSURE

In the event of a cybersecurity incident, transparency is paramount. The regulations mandate timely and accurate disclosure of incidents (four days maximum) that could potentially impact a company's operations or its investors. This requirement ensures that investors are promptly informed about cyber incidents' risks and potential consequences so they can make informed decisions about their investments.

THE CIMTRAK SOLUTION INCIDENT DETECTION AND RESPONSE

In line with the SEC's incident response requirements, CimTrak can play a crucial role by promptly identifying, reporting, and containing cybersecurity incidents. This allows organizations to take swift action, minimize damage, and fulfill regulatory obligations.

The new rules and regulations will require companies to disclose any cybersecurity incident on the new Item 1.05 of Form 8-K as well as add Regulation S-K Item 106, which will require companies to describe their processes for assessing, identifying, and managing material risks and effects from cybersecurity threats and incidents.

THE RATIONALE BEHIND THE REGULATIONS

The adoption of these regulations by the SEC is driven by several key considerations:

INVESTOR PROTECTION

The primary goal of the regulations is to protect investors' interests. By requiring companies to establish effective cybersecurity protocols and disclose incidents that could impact their financial standing, investors are better equipped to assess the risks associated with their investments.

MARKET INTEGRITY

The stability and integrity of financial markets are essential for sustainable economic growth. If left undisclosed, cyber incidents can undermine market integrity and erode investor confidence. These regulations aim to uphold market stability by promoting transparency and accountability.

RISING CYBER THREATS

With the increasing frequency and sophistication of cyberattacks, publicly traded companies have become targets for malicious actors that exploit vulnerabilities. The regulations acknowledge the evolving nature of cyber threats and provide a framework for preemptive risk management.

GLOBAL TRENDS

The SEC's move is in alignment with global trends in regulatory frameworks. Many international companies and organizations have recognized the need for enhanced transparency and cybersecurity measures, thereby encouraging collaboration and cooperation across jurisdictions.

BENEFITS AND IMPACTS

ENHANCED INVESTOR CONFIDENCE

The regulations inspire investor confidence by demonstrating that financial organizations are proactively safeguarding their investments from cyber threats. Transparent incident disclosure also enables investors to make informed decisions about their portfolios.

ELEVATED CYBERSECURITY POSTURE Companies will be incentivized to elevate their cybersecurity posture by implementing more robust risk management practices that include integrity and compliance functionality. This, in turn, reduces the likelihood of successful cyberattacks and their potential impact on operations.

STANDARDIZATION AND ACCOUNTABILITY

The regulations establish a standard framework for cybersecurity risk management and incident disclosure. This consistency streamlines compliance efforts and holds companies accountable for their cybersecurity strategies.

IDENTIFY MATERIAL CYBERSECURITY INCIDENTS

A material cybersecurity incident occurs when an organization's information systems or data security measures are compromised, resulting in unauthorized access, disclosure, alteration, or destruction of sensitive information that can negatively impact operations and the profitability of an organization.

SHIFT IN ORGANIZATIONAL CULTURE

The emphasis on cybersecurity risk management and incident disclosure could lead to a cultural shift within organizations, where cybersecurity becomes an integral part of business operations and decision-making.

The SEC's adoption of cybersecurity risk management and incident disclosure rules marks a significant stride towards a more secure and transparent financial landscape. By prioritizing investor protection, market integrity, and the recognition of evolving cyber threats, these regulations are poised to enhance both the cybersecurity posture of financial organizations and investor confidence. As the digital landscape and topography continue to evolve, these regulations serve as a beacon of accountability and resilience in the face of growing cyber risks.

THE CIMTRAK SOLUTION

CimTrak assists in maintaining compliance by offering detailed audit trails and reports. These logs demonstrate the organization's commitment to cybersecurity and can be invaluable during regulatory audits.

CIMCOR

PART 2

The Crucial Role of Integrity in Cybersecurity Threats and Incidents

As cyber threats grow in sophistication and frequency, regulators are stepping up their efforts to ensure that organizations are adequately prepared to mitigate these risks. The US Securities and Exchange Commission (SEC) has taken a significant step in this direction by introducing new cybersecurity risk management and incident disclosure rules.

These rules emphasize the principles of confidentiality, integrity, and availability—collectively known as the CIA triad —as essential components of a robust cybersecurity strategy.

INCORPORATING THE CIA TRIAD

The CIA Triad—confidentiality, integrity, and availability—has long been a cornerstone of information security. The CIA triad forms the foundation of security strategies and helps organizations assess and address risks to their information and systems. By considering these three principles, security professionals can create comprehensive security solutions that balance the need for protection against the practical requirements of data use and access.

Let's see how each principle aligns with the SEC's new rules as outlined in the **Proposed 229 CFR 229.106(a) (Regulations S-K "Item 106(a)")** and the definition of a cybersecurity incident and cybersecurity threat.

CONFIDENTIALITY

The requirement for cybersecurity risk management programs addresses the confidentiality principle directly. Companies must establish measures and controls to protect sensitive information from unauthorized access, ensuring that customer data, trade secrets, and other valuable information remain confidential.

INTEGRITY

The incident disclosure component of the rules highlights the importance of maintaining the integrity of information. Companies must provide accurate and complete details about cybersecurity incidents to ensure investors have reliable information for decision-making.

AVAILABILITY

The emphasis on board oversight highlights the availability principle. Companies must ensure that resources, including systems, personnel, and funding, are available to implement and maintain effective cybersecurity risk management practices.

CYBERSECURITY THREATS AND INTEGRITY

Cybersecurity threats encompass various malicious activities, from hacking attempts and data breaches to ransomware attacks and insider threats. Integrity is a foundational pillar in ensuring an organization's cybersecurity resilience amid this evolving threat landscape.

TRUSTWORTHINESS

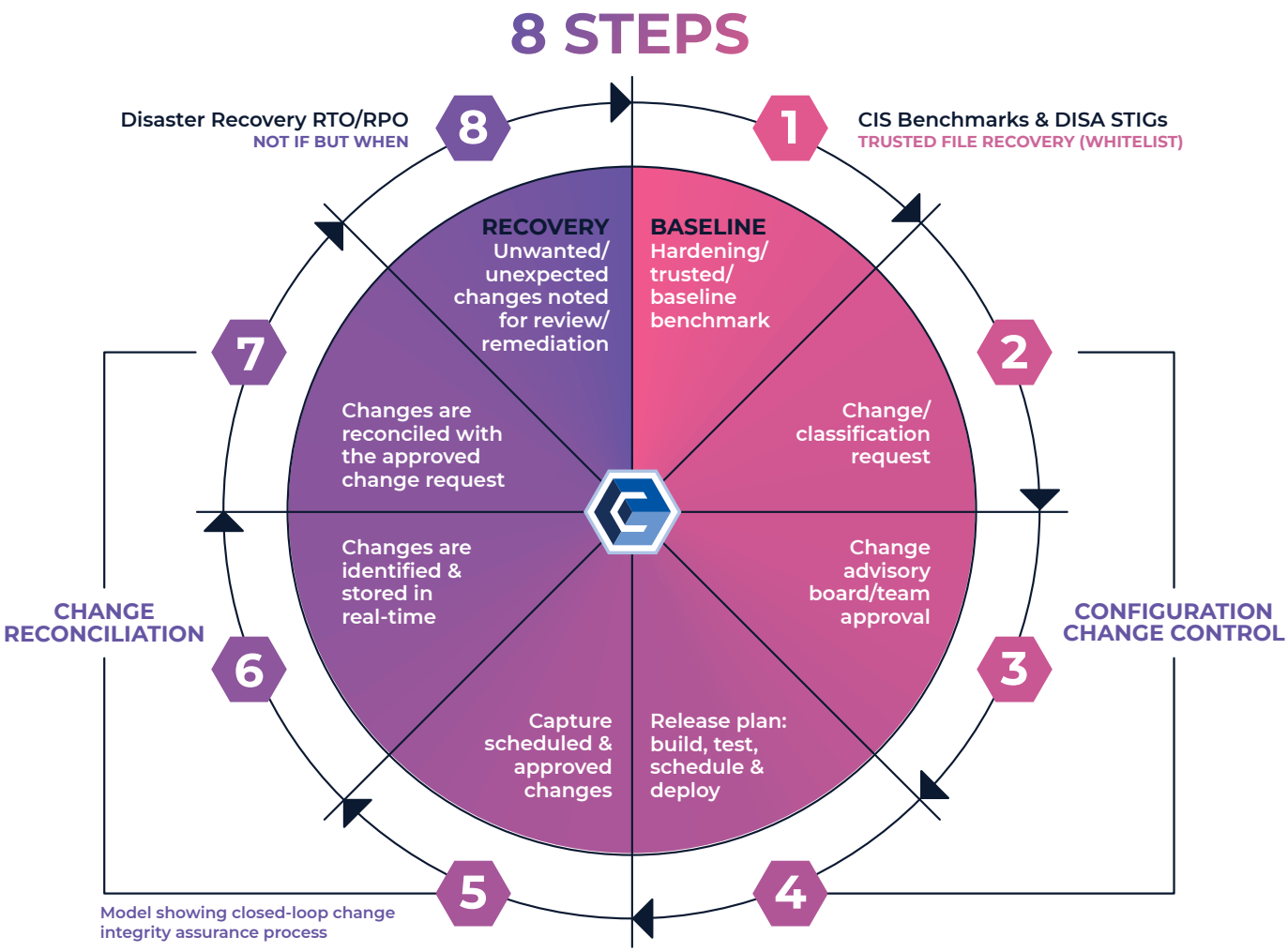
The integrity of an organization's systems, processes, and personnel directly influences its ability to fend off cyber threats. A culture of trustworthiness instills confidence in customers, investors, and partners, making it harder for threat actors to exploit vulnerabilities.

SECURE DESIGN AND IMPLEMENTATION

Integrating integrity into the design and implementation of systems/software ensures they are resistant to tampering, unauthorized access, and manipulation. Secure software development practices like code integrity checks and strong encryption can thwart potential attacks.

INSIDER THREATS

Integrity extends to personnel within an organization. Insider threats (intentional or unintentional) can have devastating consequences. Cultivating a culture of ethical behavior and accountability among employees can significantly mitigate the risk of insider-related breaches.



CYBERSECURITY INCIDENTS AND INTEGRITY

Even the most robust and well-funded cybersecurity defenses will certainly have cybersecurity incidents. When incidents occur, integrity plays a pivotal role in how organizations detect, respond, recover, and learn from these events.

TRANSPARENCY

Demonstrating integrity through transparent communication about the incident builds trust with stakeholders. Being forthcoming about the breach's impact, the steps taken to address it, and the measures implemented to prevent recurrence showcase the organization's commitment to cybersecurity and accountability.

TIMELY DETECTION & RESPONSE

Integrity shines through a timely and well-coordinated response to cybersecurity incidents. Swiftly containing the incident, notifying affected parties, and cooperating with regulatory bodies reflect an organization's dedication to minimizing damage and rectifying the situation.

CONTINUOUS IMPROVEMENT

Cybersecurity incidents serve as learning opportunities. Integrating integrity into incident response involves conducting thorough post-incident analyses, identifying vulnerabilities, and implementing corrective actions. This commitment to improvement reinforces an organization's integrity-driven approach to cybersecurity.

Integrity management (aka System Integrity Assurance) is a fundamental aspect of information security that involves maintaining data and resources' accuracy, consistency, and reliability throughout its entire life cycle. Several security controls contribute to integrity management. Here are vital controls and functionality:

DATA VALIDATION AND VERIFICATION

Input Validation: Ensuring that data entered into systems is correctly formatted and within expected ranges to prevent malicious input.
Data Verification: Using checksums, hashes, or digital signatures to confirm the integrity of transmitted or stored data.

CONFIGURATION MANAGEMENT

Baseline Configuration: Defining and maintaining a secure baseline configuration for systems and applications.
Configuration Change Monitoring: Tracking and reviewing configuration changes to prevent unauthorized modifications.

CHANGE MANAGEMENT

Version Control: Managing changes to code, configurations, and other assets to track modifications and prevent unauthorized alterations.
Change Authorization: Implementing a workflow and processes to review, approve, and document changes before they are applied.
Change Prevention: Limiting the authority of who can and cannot make changes within an operating environment to prevent malicious or circumvented processes by hackers or unauthorized personnel.

BACKUP AND RECOVERY

Regular Backups: Creating copies of data and resources to restore them in case of data loss or corruption.
Disaster Recovery Planning: Executing a process to quickly recover and restore data/service in the event of a disaster.

AUDITING AND LOGGING

Event Logging: Recording significant events and actions in a system to maintain a historical record for analysis and investigation.
Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS): Monitoring network and system activities for unauthorized or anomalous behavior.

FILE INTEGRITY MONITORING (FIM)

Continuously monitor critical system files and configurations for unauthorized changes using a FIM tool.

SYSTEM HARDENING

Utilizing configuration best practices of CIS Benchmarks or DISA STIGs to establish a foundation or root of trust.

ALLOW LISTING DATABASE

Incorporating an allowlisting database (aka whitelisting), which provides irrefutable evidence and chain of custody relative to validating and verifying if a specific set of files was developed by known and trusted software developers/companies.

STIX & TAXII FEEDS

Incorporating STIX/TAXII intelligence provides further evidence to help meet the SEC's objective of identifying cybersecurity threats.

CIMCOR

PART 3

Material Cybersecurity Incidents

In today's digitally driven world, where cyber threats are becoming increasingly sophisticated and prevalent, organizations must prioritize robust cybersecurity management and transparent incident disclosure practices. The new SEC Cybersecurity Management and Incident Disclosure Rules underpin these efforts with the concept of "material cybersecurity incident." This term, often used in legal and regulatory contexts, is pivotal in shaping an organization's response to cybersecurity incidents and their subsequent disclosure to stakeholders.

SIGNIFICANCE IN INCIDENT DISCLOSURE:

TRANSPARENCY AND TRUST

Transparently disclosing a material cybersecurity incident showcases an organization's commitment to its stakeholders' interests. By promptly sharing information about the incident, its scope, and the steps taken to mitigate the damage, the organization can maintain trust and credibility.

LEGAL AND REGULATORY OBLIGATIONS

Organizations may have legal obligations to disclose material cybersecurity incidents depending on the jurisdiction and industry. Such disclosures ensure that regulatory authorities are informed and can take appropriate action.

STAKEHOLDER COMMUNICATION

Organizations need to communicate the incidents not only to regulatory bodies but also to affected customers, partners, and investors. Providing clear and accurate information can help stakeholders understand the situation and make informed decisions.

In this section, we will explore how material cybersecurity incidents specifically pertain to the requirements of a cybersecurity incident disclosure and why understanding this concept is crucial for public companies (registrants).

DEFINING A MATERIAL CYBERSECURITY INCIDENT

A cybersecurity incident involves the compromise of sensitive information or critical systems of a registrant that could impact an organization's operations, reputation, or financial stability.

So, what is a material cybersecurity incident, and what is the new reporting requirement? It is important to note that what constitutes a material cybersecurity incident may vary based on the industry, the nature of the data or systems compromised, and relevant legal and regulatory frameworks.

The new SEC regulation entitled Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure has added provisions that required a modification to Form 8-K, incorporating Item 1.05, titled "Material Cybersecurity Incidents." This change mandates that a registrant must submit a Form 8-K within four business days of determining that a cybersecurity incident is material.

A registrant may delay filing if the United States Attorney General ("Attorney General") determines immediate disclosure would pose a substantial risk to national security or public safety. *[Note that a foreign issuer (FPI), other than a foreign government, may have other reporting obligations (e.g., Form 20-F and Form 6-K); however, that is beyond the scope of this article]*.

Once a cybersecurity incident has occurred, a registrant must proceed as soon as reasonably practical after discovery of the incident to determine whether it is material. This requirement also obligates the registrant to account for incidents occurring both internally and within third-party service providers, including cybersecurity incidents that can arise unintentionally or because of a deliberate attack. Reporting should include a description of the nature, scope, and timing of the incident and the impact or reasonably likely impact. Registrants must amend a prior Item 1.05 Form 8–K to disclose any information called for in Item 1.05(a) that was not determined or was unavailable at the time of the initial Form 8–K filing.

Item 1.05 of Form 8-K references 17 CFR 229.106 (item 106), which defines a cybersecurity incident as an unauthorized occurrence, or a series of related unauthorized occurrences, on or conducted through a registrant's information systems that jeopardizes the confidentiality, integrity, or availability of a registrant's information systems or any information residing therein. Furthermore, the SEC Cybersecurity disclosure final rule defines "information systems" as electronic information resources owned or used by the registrant, including physical or virtual infrastructure controlled by such information resources, or components thereof, organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of the registrant's information to maintain or support the registrant's operations.

When evaluating materiality, the registrant must maintain objectivity and consider all pertinent quantitative and qualitative factors. The SEC explains that the "materiality" standard to be applied should be consistent with the numerous cases on the subject, including but not limited to:

- Matrixx Initiatives, Inc. v. Siracusano (563 U.S. 27 (2011))
- Basic, Inc. v. Levinson (485 U.S. 224, 232 (1988))
- TSC Industries, Inc. v. Northway, Inc. (426 U.S. 438, 449 (1976))

Additionally, consideration should also be given to the standards outlined in 17 CFR 230.405 ("Securities Act Rule 405") and 17 CFR 240.12b–2 ("Exchange Act Rule 12b–2"). That is, information is material if "there is a substantial likelihood that a reasonable shareholder would consider it important" in making an investment decision or if it would have "significantly altered the 'total mix' of information made available." "Doubts as to the critical nature" of the relevant information should be "resolved in favor of those the statute is designed to protect," namely investors. Certainly, a matter is material if there is evidence that a shareholder or investor would consider it important in making an investment decision and if disclosing the information would have altered the investor's views or decisions. Suggesting the importance of any compromised information should be considered, along with the impact it would have on the company's operations and profitability.

Factors to consider when assessing materiality should include matters such as the following:

- Registrant's reputation and competitive position
- The potential for legal action or regulatory investigations
- The possibility of an adverse outcome
- The potential degree and/or consequence of the loss
- Continued trust by both customers and vendor relationships

THE CIMTRAK SOLUTION DEMONSTRABLE ACCOUNTABILITY

CimTrak's comprehensive reporting capabilities help organizations provide evidence of their cybersecurity measures to regulatory bodies. This transparency enhances trust among investors, stakeholders, and regulators alike.

CIMCOR

PART 4

The Price of Insecurity

HOW CYBERSECURITY BREACHES IMPACT STOCK PRICES AND THE NEW SEC CYBERSECURITY RULING

The consequences of a cybersecurity breach extend beyond compromised data and damaged reputation; they can also significantly impact a publicly traded company's stock price. This section will explore how cybersecurity breaches can negatively impact stock prices and the Securities and Exchange Commission's (SEC) new cybersecurity ruling, which aims to address this growing threat.

THE CONNECTION BETWEEN CYBERSECURITY INCIDENTS AND STOCK PRICES

IMMEDIATE STOCK PRICE DROP

When a company experiences a cybersecurity breach, it often leads to an instant drop in its stock price. Investors panic as they fear the potential financial and reputational damage that can follow such incidents. This drop can be substantial, depending on the severity of the breach and the company's response.

LOSS OF CUSTOMER TRUST

Cybersecurity breaches erode customer trust, which can result in reduced revenues. Customers worry about the safety of their data and may take their business elsewhere. This loss of revenue and potential long-term damage to the customer base can further depress a company's stock price.

LEGAL AND REGULATORY COSTS

Dealing with the aftermath of a breach involves significant legal and regulatory costs. Companies may face fines, lawsuits, and the expense of implementing new security measures. These costs can negatively impact a company's financial health and, subsequently, its stock price.

REPUTATION DAMAGE

The impact on a company's reputation can be long-lasting. Investors take into account a company's brand image, and a tarnished reputation can lead to a loss of shareholder confidence, resulting in a decline in stock value.

OPERATIONAL DISRUPTION

Cybersecurity breaches can disrupt a company's operations, causing downtime and affecting production. This disruption can result in lower revenue and profitability, causing investors to reevaluate the company's stock.

THE SEC'S NEW CYBERSECURITY RULING & FINANCIAL IMPACT

Recognizing the increasing threat that cybersecurity breaches pose to investors and the financial markets, the SEC introduced new cybersecurity disclosure requirements. These requirements aim to enhance transparency and help investors make informed decisions regarding the cybersecurity risks associated with their investments as determined by the shortfall in stock prices and dividends. Another financial impact often comes in the form of penalties for negligence and non-compliance. Specific to the new SEC rules, there are currently no formal details of penalties or repercussions for failing to meet either of the two requirements of Cyber Risk Management and Incident Disclosure. However, it is expected that this may change in the near future.

KEY ASPECTS OF THE SEC'S CYBERSECURITY RULING

ENHANCED DISCLOSURES

Publicly traded companies are now required to provide more detailed disclosures about their cybersecurity risks and incidents in their annual and quarterly reports, as well as an 8-K, four days following the time in which they learn of the cybersecurity event, including information on the potential financial and operational impact of breaches.

TIMELY REPORTING

Companies must promptly report material cybersecurity incidents to the SEC and investors, ensuring that investors receive timely information about potential risks.

BOARD OVERSIGHT

The SEC encourages companies to have board-level oversight of cybersecurity risk management. This signals the importance of cybersecurity at the highest levels of an organization.

INTERNAL CONTROLS

Companies are expected to establish and maintain effective internal controls to assess and mitigate cybersecurity risks.

IMPACT ON STOCK PRICES

An example of how a cybersecurity breach can negatively impact the stock price of a publicly traded company can be seen in the recent MGM casino cyber-attack. On Friday, just hours before the attack, MGM Resorts International closed on the NYSE (MGM) at 43.74 with a market cap of $15.35B. Today (9/25/23), MGM is trading at 36.74 with a market cap of $12.9B. This breach represents a loss in market cap of 16%, which equates to $2.45B.

Another recent event that is testing the new SEC disclosure requirements is Clorox. On August 14th, Clorox disclosed on its website that it had been the victim of a hack that impacted several critical systems. Since then, Clorox has also filed an 8-K. Weeks later, Clorox further stated that it had to resort to manual processes while systems were being repaired, resulting in fewer orders being processed, which means fewer Clorox products are making their way to stores.

Cybersecurity breaches pose a significant threat to publicly traded companies, with significant potential to negatively impact their stock prices. The SEC's new cybersecurity ruling represents a crucial step toward addressing these risks by increasing transparency, accountability, and investor protection. Investors and companies alike must recognize the growing importance of cybersecurity in today's interconnected world and adapt their strategies accordingly to safeguard their data and investments.

MGM RESORTS INTERNATIONAL™

▼ $2.45B
LOSS IN MARKET CAP

Las Vegas Review-Journal has estimated that MGM Resorts International is losing between $4.2 million and $8.4 million in daily revenue and around $1 million in cash flow every day. More details will surface as MGM is going to file an 8-K notice with the SEC, given that the event has a material effect on their businesses.

CLOROX

▼ $3.42B
LOSS IN MARKET CAP

The stock price of Clorox has fallen from 160.17 (8/14/23) to 132.32 (9/25/23). This breach represents a loss in market cap of 17%, which equates to $3.42B.

HOW TO PREPARE AND COMPLY

To ensure compliance with the new SEC cybersecurity ruling, organizations need to ensure they are prepared to meet the new requirements. Here are some essential steps for compliance preparation:

ASSESS YOUR CYBERSECURITY PROGRAM

Conduct a thorough assessment of your organization's cybersecurity program to identify any gaps or weaknesses. This assessment should encompass risk assessments, incident response plans, employee training, and vendor management. Update any outdated policies, procedures, and measures to strengthen your cybersecurity posture.

ENHANCE INCIDENT RESPONSE CAPABILITIES

Implement or improve your incident response plan to ensure it aligns with the new reporting requirements. Work on reducing the time it takes to detect, respond to, and recover from cyber incidents.

ESTABLISH STRONG GOVERNANCE

Ensure that your cybersecurity governance structure is robust and well-documented. This includes clear roles and responsibilities for cybersecurity within the organization and regular board-level oversight.

ENGAGE EXECUTIVES AND BOARDS

Cybersecurity should be a top priority for executives and boards, and they must be actively involved in the decision-making process. Regular reporting and updates on cybersecurity matters should be part of the board's agenda.

USE SOPHISTICATED TOOLS

Investing in an IT security tool, such as CimTrak, can help organizations identify threats before they hit. CimTrak can provide real-time monitoring, track and remediate changes, and offer audit-ready forensic reporting, making it easier to comply with the new SEC ruling and meet the stringent four-day timeline.

CIMCOR

PART 5

How CimTrak Can Help

CIMTRAK PROVIDES

TIMELY DETECTION

CimTrak's real-time monitoring capabilities enable organizations to identify and mitigate breaches promptly. This quick detection is vital for initiating an effective response and ensuring timely disclosure.

FORENSIC ANALYSIS

CimTrak's data and logs can be instrumental in conducting a thorough forensic analysis in the aftermath of a cybersecurity incident. This analysis aids in understanding the scope of the breach, the vulnerabilities exploited, and the potential impact.

DOCUMENTATION FOR COMPLIANCE

Regulatory bodies often require organizations to demonstrate their efforts to maintain cybersecurity controls and promptly disclose incidents. CimTrak's comprehensive monitoring and reporting features provide the necessary documentation to meet these compliance requirements.

CONFIGURATION & CHANGE MANAGEMENT

CimTrak maintains a detailed inventory of configurations, ensuring that any unauthorized or unexpected changes are immediately identified and addressed. This capability is crucial in preventing attackers from gaining access through misconfigurations or changes resulting from malicious or unintentional modifications.

POLICY ENFORCEMENT

CimTrak helps organizations enforce cybersecurity policies by ensuring that systems and applications adhere to predefined security configurations and policies. This minimizes the risk of security gaps and reduces the attack surface.

VULNERABILITY MANAGEMENT

CimTrak's ability to detect and mitigate breaches swiftly helps reduce the potential damage caused by the incident. This, in turn, contributes to preserving the organization's reputation, customer trust, and financial impact.

CIMCOR

PART 6

Resources & References

www.sec.gov/files/rules/final/2023/33-11216.pdf

https://www.federalregister.gov/documents/2023/08/04/2023-16194/cybersecurity-risk-management-strategy-governance-and-incident-disclosure

https://www.sec.gov/news/press-release/2023-139

https://www.reviewjournal.com/business/casinos-gaming/analyst-mgm-losing-4-2m-8-4m-a-day-because-of-cyberattack-2906379/

https://www.wsj.com/articles/clorox-cyberattack-brings-early-test-of-new-sec-cyber-rules-b320475

DISCLAIMER

This report is only a brief summary of the new Cybersecurity Risk SEC rule and does not constitute legal advice. Should you encounter a situation that constitutes a Cybersecurity Incident or any matter touched upon in this document, you should consult with legal counsel having experience in this area of the law and not rely on the information provided in this document.

SUPPORTED PLATFORMS

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS XP, Vista, 7, 8, 10, 11, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise, Windows 11 IoT Enterprise
WINDOWS SERVER 2003, 2008, 2012, 2016, 2019, 2022
LINUX Alma, Amazon, ARM, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, Rocky, SUSE, Ubuntu, others
FreeBSD 12, 13
SUN SOLARIS x86/SPARC
MacOS 5, 6, 7, 8, 9, 10, 11
HP-UX Itanium, PA-RISC
AIX 6.1, 7.1, 7.2, 7.3

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES Compressed, hidden, offline, read-only, archive, reparse point, Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Arista, Aruba, Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Palo Alto, Sophos, others

Supported Platforms CimTrak For Databases

IBM DB2, Microsoft SQL Server, MySQL, Oracle
PARAMETERS MONITORED Default Rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored Procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Amazon AWS, Google Cloud, Microsoft Azure

Supported Container & Orchestration Integrations

Amazon Elastic Kubernetes Service (EKS), Docker, Docker Enterprise, Google Kubernetes Engine (GKE), Kubernetes, Podman

Supported Ticketing Integrations

Atlassian Jira, BMC Remedy, CA ServiceDesk, ServiceNow

Supported SIEM Integrations

IBM QRadar, LogRhythm, McAfee Event Security Manager, Microfocus Arcsight, Splunk, others

Supported Under CimTrak's Trusted File Registry™

CentOS 7, Microsoft Windows 7, 8, 8.1, 10, 11, XP, 2003, 2008, 2012, 2016, 2019, 2022, Oracle Linux 7, Redhat Enterprise Linux 7

SUPPORTED BENCHMARKS

ALIBABA
ALMA
AMAZON ELASTIC KUBERNETES
AMAZON LINUX
APACHE
APPLE MAC OS
AZURE
CENTOS
CISCO Firewall, IOS
DEBIAN
DISTRIBUTION INDEPENDENT
FEDORA
GOOGLE Chrome, Container, Kubernetes
IBM
KUBERNETES
MICROSOFT Access, Edge, Excel, IIS, Intune, Office, PowerPoint, SharePoint, SQL, Windows, Windows Server, Word
MONGODB
NGINX
ORACLE Cloud, Database, Linux, MySQL
PALO ALTO
POSTGRESQL
RED HAT
RHEL8
ROCKY
ROS
SUSE
UBUNTU LXD, Linux
VMWARE

CIMCOR

Cimcor develops innovative, next-generation, file integrity monitoring software. The CimTrak Integrity Suite monitors and protects a wide range of physical, network, cloud, and virtual IT assets in real-time, while providing detailed forensic information about all changes. Securing your infrastructure with CimTrak helps you get compliant and stay that way.

REQUEST A DEMO

CIMTRAK

CIMCOR.COM | FOLLOW US @CIMTRAK