CYBR2100 Final Policy Memo

Molson Coors Cyberattack

Prepared by: Clayton Holden, CIO, Molson Coors Beverage Company
Date: October 10th, 2025

Executive Summary

In March 2021, Molson Coors was hit with a ransomware attack that shut down brewing, logistics, and corporate systems across the company for nearly two weeks. The attack started when a contractor with a Molson Coors email account opened a malicious email. That one email launched a worm that spread through the network and encrypted data everywhere it touched. The shutdown stopped production and shipments in the U.S., Canada, and the U.K. and caused about $120–$140 million in deferred earnings. It's still unclear if a ransom was ever paid (most likely was). Operations were back online by late March, and production losses were recovered later that year, but the event showed serious weak points, especially in vendor oversight, employee awareness, and network separation between IT and production

CYBR2100 Final Policy Memo

Molson Coors Cyberattack

Prepared by: Clayton Holden, CIO, Molson Coors Beverage Company
Date: October 10th, 2025

Executive Summary

In March 2021, Molson Coors was hit with a ransomware attack that shut down brewing, logistics, and corporate systems across the company for nearly two weeks. The attack started when a contractor with a Molson Coors email account opened a malicious email. That one email launched a worm that spread through the network and encrypted data everywhere it touched. The shutdown stopped production and shipments in the U.S., Canada, and the U.K. and caused about $120–$140 million in deferred earnings. It's still unclear if a ransom was ever paid (most likely was). Operations were back online by late March, and production losses were recovered later that year, but the event showed serious weak points, especially in vendor oversight, employee awareness, and network separation between IT and production systems. The main fix

is a full Security & Operations Policy Framework that tightens authorization, limits vendor access, and makes communication during incidents faster and clearer so future threats are handled the right way.

Incident Report

What Went Wrong

The 2021 cyberattack started when a contractor with a Molson Coors corporate email fell for a social-engineering email and opened an attachment that dropped malware into our network. The malware acted like a worm, spreading across systems and encrypting everything from file servers to production controllers. That forced an immediate shutdown of all brewing and shipping operations. Employees couldn't log in or access production schedules or shipment tools. Forensics later confirmed it was ransomware. Multiple file servers were locked, and restoring systems took roughly two weeks.

From a technical side, our main issue was the lack of strong segmentation between corporate IT and operational technology. Once the malware got in, it moved freely because of shared credentials and weak access boundaries. Our IT team reacted fast and shut systems down, but without clear roles defined ahead of time, containment wasn't coordinated and downtime dragged out longer than it needed to.

From a legal and ethical view, Molson Coors met disclosure rules by filing a Form 8-K with the SEC within 48 hours. But internally, communication didn't move as fast. Employees and distributors heard about the attack through news outlets before we sent out an internal message.

Ethical & Legal Framework

Using a duty-based approach, the company has an obligation to protect systems and communicate honestly with everyone affected. We met the basic legal standards, but ethically, the duty of care fell short, especially for employees who lost hours or customers stuck waiting for products. It shows how a technical problem can quickly turn into a people problem.

Laws and frameworks applied:

- CFAA (18 U.S.C. §1030): Prevent and respond to unauthorized access.
- NIST Incident Response Lifecycle: Prepare -> Detect -> Contain -> Eradicate -> Recover -> Learn.
- SOX & SEC Disclosure Rules: Require quick, accurate reporting of material cybersecurity events.

Authorization Boundary

During the attack, IT Security and Infrastructure reported directly to the CIO, who approved the full shutdown. Brewery managers were informed after the fact, which caused confusion. Going forward, all containment actions will include real-time coordination between IT, OT, Legal, and Communications through a pre-approved chain of command.

NIST Lifecycle Tie-In

- Preparation: Weak network segmentation; no tabletop drills.
- Detection & Analysis: Found fast but lacked automated correlation tools.
- Containment: Quick but messy; took down more systems than needed.
- Eradication & Recovery: Forensic teams and IT staff restored systems in about two weeks.
- Lessons Learned: Need integrated response planning, better authorization mapping, and real-time transparency.

Security & Operations Policy Framework

Acceptable Use Policy

All employees and contractors must:

- Access systems only with approved credentials and multi-factor authentication.
- Never connect personal devices or USB drives to company networks.
- Complete yearly cybersecurity and ethics training covering phishing, passwords, and data privacy.
- Report anything suspicious within 30 minutes to the Security Operations Center.

Violations can lead to suspension or termination.

Monitoring & Retention Clause

- Purpose: Detect threats and meet compliance standards while respecting privacy.

- Scope: Monitor network logs, system telemetry, and production data for security purposes only.

- Data Minimization: Only collect what’s needed for detection. Avoid personal content or employee messages.

- Retention: Keep logs for 180 days; preserve investigation evidence for up to one year.

- Evidence Handling: Hash all evidence with SHA-256 and store it on encrypted, access-controlled servers.

- Privacy & Compliance: Meets GDPR, CCPA, and state laws; ensures proportional and necessary data use.

Coordinated Disclosure Plan

1. Internal Notice: Within 24 hours, notify senior leadership, Legal, and HR.

2. Regulatory Reporting: File required disclosures (SEC 8-K, state AG notices) within 72 hours.

3. Stakeholder Notice: Inform employees, distributors, and partners through internal channels before the public announcement.

4. Public Statement: Release confirmed updates once containment and investigation are stable.

5. External Coordination: Work with CISA, FBI, and ISAC partners to share indicators of compromise.

Rules of Engagement

- Scope: Testing and incident response limited to approved systems and sandboxes.

- Consent: No scans or testing without written approval from the CIO and OT Director.

- Deconfliction: Give at least 24 hours’ notice before planned outages or testing.

- Stop-Test: Halt immediately if a live production system is affected. Escalate to the Incident Manager.

- Roles: SOC Analysts detect; OT Managers confirm scope; CIO authorizes containment.

AI Use in Security Operations

- Purpose: Use AI to support analysts, not replace them.
- Transparency: Every AI alert shows a plain-language reason and confidence score.
- Human Review: A human analyst confirms high-impact actions before enforcement.
- Appeals: Employees can challenge bad alerts through IT Security. All appeals answered in 24 hours, resolved within five business days.
- Data Handling: AI only analyzes anonymized data. No personal content or emails.
- Retraining: Update AI models every six months; quarterly reports on accuracy and false positives go to leadership.

Production Network Segmentation & Backup Policy

- Network Segmentation: Physically and logically separate OT from IT using VLANs and firewalls.
- Access Controls: OT admin accounts must use unique credentials, not tied to corporate Active Directory.
- Backups: Keep daily encrypted backups offline, tested monthly.
- Recovery Goals: RTO < 48 hours, RPO < 12 hours for production systems.

Controls and Trade-Offs

Fixing the Root Causes

This new framework covers the weak spots the attack exposed:

- Unclear Authorization: ROE and disclosure plan define who approves what.
- Poor Segmentation: New network rules isolate OT from IT to stop lateral spread.

- Limited Monitoring: AI-assisted alerts expand visibility while keeping a human in charge.

- Communication Gaps: The disclosure plan makes sure employees and partners hear it directly from us first.

- Evidence Handling: New retention and hashing rules protect the integrity of what we collect.

Trade-Offs

- Privacy vs. Monitoring: Collecting security data helps defend the network but risks overreach. The minimum-necessary rule and anonymization keep it fair.

- Speed vs. Oversight: Human review may slow response a bit but avoids false lockouts.

- Cost vs. Security: Segmentation and AI audits cost money, but they meet insurance and ethical duty-of-care expectations.

- Operations vs. Control: More approvals could slow maintenance, but the clear escalation process keeps things moving.

Implementation Timeline

Phase	Duration	Milestones
Phase 1 - Policy Rollout and Training	**60 Days**	**Publish AUP and disclosure plan, train all mangers**
Phase 2 - Technical Controls	**90 Days**	**Install segmentation, verify backups, and set up AI reviews**
Phase 3 - Review and Audit	**180 Days**	**Run tabletop exercise, update metrics, report to Audit Committee**

Ethical & Legal Link

This plan supports beneficence and justice. Legally, it keeps us compliant with SEC disclosure rules, CFAA, and state breach laws. The fixes are balanced, they manage real risk without invading privacy or slowing operations unnecessarily.

Conclusion

The 2021 Molson Coors ransomware attack changed how we look at security in manufacturing. It showed that production networks need the same attention and protection as finance or HR systems. This new Security & Operations Framework closes the gaps with stronger authorization, transparent communication, responsible AI use, and ethical data practices.

Big picture, regulators should push all large manufacturers to maintain clear incident response authority and disclosure timelines, just like financial institutions do. Inside Molson Coors, we'll review this framework every six months, audit for compliance, and update it yearly. The goal is simple: next time something like this happens, we'll respond faster, stay transparent, and protect both our operations and our people.

References

- Molson Coors Beverage Co. SEC Form 8-K, March 11 2021 – disclosure of cybersecurity incident.

- Molson Coors Press Release, March 26 2021 – update on systems restoration.

- BleepingComputer. *Molson Coors Brewing Operations Disrupted by Cyberattack.* March 11 2021.

- CPO Magazine. *Suspected Ransomware Attack Shuts Down Molson Coors.* March 19 2021.

- SecureWorld News. *Molson Coors Still Recovering, Counting Cost of Data Breach.* April 5 2021.

- NIST SP 800-61 Rev.2: *Computer Security Incident Handling Guide.*

- Weber, Ed. *Ethics in Technology* (2024), Chs. 4 & 11 – Duty of Care & AI Ethics.

Acknowledgments

Special thanks to Justin Holden and Austin, both employees at Molson Coors, for taking the time to share their firsthand experiences and insights from the 2021 incident. Their input helped me better understand the real impact of this event and how response efforts looked on the ground.

systems. The main fix is a full Security & Operations Policy Framework that tightens authorization, limits vendor access, and makes communication during incidents faster and clearer so future threats are handled the right way.

Incident Report

What Went Wrong

The 2021 cyberattack started when a contractor with a Molson Coors corporate email fell for a social-engineering email and opened an attachment that dropped malware into our network. The malware acted like a worm, spreading across systems and encrypting everything from file servers to production controllers. That forced an immediate shutdown of all brewing and shipping operations. Employees couldn’t log in or access production schedules or shipment tools. Forensics later confirmed it was ransomware. Multiple file servers were locked, and restoring systems took roughly two weeks.

From a technical side, our main issue was the lack of strong segmentation between corporate IT and operational technology. Once the malware got in, it moved freely because of shared credentials and weak access boundaries. Our IT team reacted fast and shut systems down, but without clear roles defined ahead of time, containment wasn’t coordinated and downtime dragged out longer than it needed to.

From a legal and ethical view, Molson Coors met disclosure rules by filing a Form 8-K with the SEC within 48 hours. But internally, communication didn’t move as fast. Employees and distributors heard about the attack through news outlets before we sent out an internal message.

Ethical & Legal Framework

Using a duty-based approach, the company has an obligation to protect systems and communicate honestly with everyone affected. We met the basic legal standards, but ethically, the duty of care fell short, especially for employees who lost hours or customers stuck waiting for products. It shows how a technical problem can quickly turn into a people problem.

Laws and frameworks applied:

- CFAA (18 U.S.C. §1030): Prevent and respond to unauthorized access.
- NIST Incident Response Lifecycle: Prepare -> Detect -> Contain -> Eradicate -> Recover -> Learn.
- SOX & SEC Disclosure Rules: Require quick, accurate reporting of material cybersecurity events.

Authorization Boundary

During the attack, IT Security and Infrastructure reported directly to the CIO, who approved the full shutdown. Brewery managers were informed after the fact, which caused confusion. Going forward, all containment actions will include real-time coordination between IT, OT, Legal, and Communications through a pre-approved chain of command.

NIST Lifecycle Tie-In

- Preparation: Weak network segmentation; no tabletop drills.
- Detection & Analysis: Found fast but lacked automated correlation tools.
- Containment: Quick but messy; took down more systems than needed.
- Eradication & Recovery: Forensic teams and IT staff restored systems in about two weeks.
- Lessons Learned: Need integrated response planning, better authorization mapping, and real-time transparency.

Security & Operations Policy Framework

Acceptable Use Policy

All employees and contractors must:

- Access systems only with approved credentials and multi-factor authentication.
- Never connect personal devices or USB drives to company networks.
- Complete yearly cybersecurity and ethics training covering phishing, passwords, and data privacy.

- Report anything suspicious within 30 minutes to the Security Operations Center.

Violations can lead to suspension or termination.

Monitoring & Retention Clause

- Purpose: Detect threats and meet compliance standards while respecting privacy.
- Scope: Monitor network logs, system telemetry, and production data for security purposes only.
- Data Minimization: Only collect what's needed for detection. Avoid personal content or employee messages.
- Retention: Keep logs for 180 days; preserve investigation evidence for up to one year.
- Evidence Handling: Hash all evidence with SHA-256 and store it on encrypted, access-controlled servers.
- Privacy & Compliance: Meets GDPR, CCPA, and state laws; ensures proportional and necessary data use.

Coordinated Disclosure Plan

6. Internal Notice: Within 24 hours, notify senior leadership, Legal, and HR.
7. Regulatory Reporting: File required disclosures (SEC 8-K, state AG notices) within 72 hours.
8. Stakeholder Notice: Inform employees, distributors, and partners through internal channels before the public announcement.
9. Public Statement: Release confirmed updates once containment and investigation are stable.
10. External Coordination: Work with CISA, FBI, and ISAC partners to share indicators of compromise.

Rules of Engagement

- Scope: Testing and incident response limited to approved systems and sandboxes.

- Consent: No scans or testing without written approval from the CIO and OT Director.

- Deconfliction: Give at least 24 hours' notice before planned outages or testing.

- Stop-Test: Halt immediately if a live production system is affected. Escalate to the Incident Manager.

- Roles: SOC Analysts detect; OT Managers confirm scope; CIO authorizes containment.

AI Use in Security Operations

- Purpose: Use AI to support analysts, not replace them.

- Transparency: Every AI alert shows a plain-language reason and confidence score.

- Human Review: A human analyst confirms high-impact actions before enforcement.

- Appeals: Employees can challenge bad alerts through IT Security. All appeals answered in 24 hours, resolved within five business days.

- Data Handling: AI only analyzes anonymized data. No personal content or emails.

- Retraining: Update AI models every six months; quarterly reports on accuracy and false positives go to leadership.

Production Network Segmentation & Backup Policy

- Network Segmentation: Physically and logically separate OT from IT using VLANs and firewalls.

- Access Controls: OT admin accounts must use unique credentials, not tied to corporate Active Directory.

- Backups: Keep daily encrypted backups offline, tested monthly.

- Recovery Goals: RTO < 48 hours, RPO < 12 hours for production systems.

Controls and Trade-Offs

Fixing the Root Causes

This new framework covers the weak spots the attack exposed:

- Unclear Authorization: ROE and disclosure plan define who approves what.
- Poor Segmentation: New network rules isolate OT from IT to stop lateral spread.
- Limited Monitoring: AI-assisted alerts expand visibility while keeping a human in charge.
- Communication Gaps: The disclosure plan makes sure employees and partners hear it directly from us first.
- Evidence Handling: New retention and hashing rules protect the integrity of what we collect.

Trade-Offs

- Privacy vs. Monitoring: Collecting security data helps defend the network but risks overreach. The minimum-necessary rule and anonymization keep it fair.
- Speed vs. Oversight: Human review may slow response a bit but avoids false lockouts.
- Cost vs. Security: Segmentation and AI audits cost money, but they meet insurance and ethical duty-of-care expectations.
- Operations vs. Control: More approvals could slow maintenance, but the clear escalation process keeps things moving.

Implementation Timeline

Phase	Duration	Milestones
Phase 1 - Policy Rollout and Training	**60 Days**	**Publish AUP and disclosure plan, train all mangers**
Phase 2 - Technical Controls	**90 Days**	**Install segmentation, verify backups, and set up AI reviews**

Phase 3 - Review and Audit	**180 Days**	**Run tabletop exercise, update metrics, report to Audit Committee**

Ethical & Legal Link

This plan supports beneficence and justice. Legally, it keeps us compliant with SEC disclosure rules, CFAA, and state breach laws. The fixes are balanced, they manage real risk without invading privacy or slowing operations unnecessarily.

Conclusion

The 2021 Molson Coors ransomware attack changed how we look at security in manufacturing. It showed that production networks need the same attention and protection as finance or HR systems. This new Security & Operations Framework closes the gaps with stronger authorization, transparent communication, responsible AI use, and ethical data practices.

Big picture, regulators should push all large manufacturers to maintain clear incident response authority and disclosure timelines, just like financial institutions do. Inside Molson Coors, we'll review this framework every six months, audit for compliance, and update it yearly. The goal is simple: next time something like this happens, we'll respond faster, stay transparent, and protect both our operations and our people.

References

- Molson Coors Beverage Co. SEC Form 8-K, March 11 2021 – disclosure of cybersecurity incident.

- Molson Coors Press Release, March 26 2021 – update on systems restoration.

- BleepingComputer. *Molson Coors Brewing Operations Disrupted by Cyberattack.* March 11 2021.

- CPO Magazine. *Suspected Ransomware Attack Shuts Down Molson Coors.* March 19 2021.

- SecureWorld News. *Molson Coors Still Recovering, Counting Cost of Data Breach.* April 5 2021.

- NIST SP 800-61 Rev.2: *Computer Security Incident Handling Guide.*
- Weber, Ed. *Ethics in Technology* (2024), Chs. 4 & 11 – Duty of Care & AI Ethics.

Acknowledgments

Special thanks to Justin Holden and Austin, both employees at Molson Coors, for taking the time to share their firsthand experiences and insights from the 2021 incident. Their input helped me better understand the real impact of this event and how response efforts looked on the ground.