Cybersecurity Risk in the Supply Chain: Case Studies of Chipotle and TSMC

Purna Chandra Subhash Veeravalli

SCM 563 – Purchasing and Supply Management

Professor David Cantor

Contents

1. Abstract

This paper examines the critical role of cybersecurity in today's interconnected business environment, focusing on the significant breaches at Chipotle Mexican Grill and Taiwan Semiconductor Manufacturing Company (TSMC). It delves into the factors contributing to these cyber-attacks, their impacts on the companies' operations, finances, and reputations, and the lessons learned to enhance cybersecurity practices. The analysis explores how vulnerabilities in payment systems and supply chain operations can expose firms to cyber risks, emphasizing the importance of proactive measures. By studying these cases, the paper underscores the necessity of robust cybersecurity frameworks, supplier evaluation, and regulatory compliance in mitigating threats and safeguarding organizational assets.

2. Introduction

In today's digital age, cybersecurity has become a critical concern for organizations across all industries. The increasing complexity of global supply chains, reliance on technology, and interconnected systems have amplified the risk of cyber-attacks. Two significant cases—the 2017 payment card breach at Chipotle Mexican Grill and the 2018 malware outbreak at Taiwan Semiconductor Manufacturing Company (TSMC)—highlight the severe consequences of cybersecurity vulnerabilities. These incidents not only disrupted operations but also impacted financial performance and customer trust.

Chipotle Mexican Grill operates over 2,250 restaurants across North America, specializing in fast-casual Mexican-inspired cuisine. Its operations depend heavily on supply chain networks for sourcing ingredients such as sustainably raised meats from Niman Ranch, as well as third-party services like payment processors and delivery systems. In 2017, malware infiltrated its point-of-sale (POS) systems through vulnerabilities in third-party managed systems, compromising customer payment data across all its locations. The breach exposed sensitive information, leading to regulatory scrutiny and customer concerns. In its SEC filings, Chipotle disclosed the breach, outlining mitigation steps, such as removing the malware and enhancing security protocols. This incident emphasized the risks posed by supplier-managed systems and the need for robust cybersecurity measures across its supply chain.

Taiwan Semiconductor Manufacturing Company (TSMC) is a global leader in semiconductor manufacturing, supplying chips to major technology companies like Apple, Nvidia, and Qualcomm. TSMC's operations rely on extensive supplier relationships, including KLA Corp for quality control, ASML for lithography equipment, and SUMCO for silicon wafers. In 2018, a cyber-attack introduced by a third-party equipment supplier spread malware throughout its production network, disrupting operations and causing shipment delays that resulted in an $85 million financial loss. The breach was detailed in SEC filings, where TSMC outlined corrective actions, such as improved firewall protections and automated system checks. This incident underscored the vulnerabilities in supplier interactions and the cascading impact on operations and revenues.

This paper explores the contributing factors, supply chain vulnerabilities, and regulatory disclosures of these breaches, offering actionable recommendations to strengthen cybersecurity frameworks in increasingly interconnected global networks.

3. Research Objective

This paper seeks to address the following research question: What are the primary factors that led to the cybersecurity breaches at Chipotle and TSMC, and what proactive strategies can companies implement to mitigate these risks, particularly in their supply chains?

• Cybersecurity Challenges at Chipotle

Chipotle Mexican Grill faces the critical challenge of protecting its point-of-sale (POS) systems and customer data from cyberattacks. A previous breach allowed attackers to install malware on its payment systems, compromising sensitive customer information like credit card details. The company’s primary problem is ensuring the security of its payment infrastructure while complying with data protection regulations.

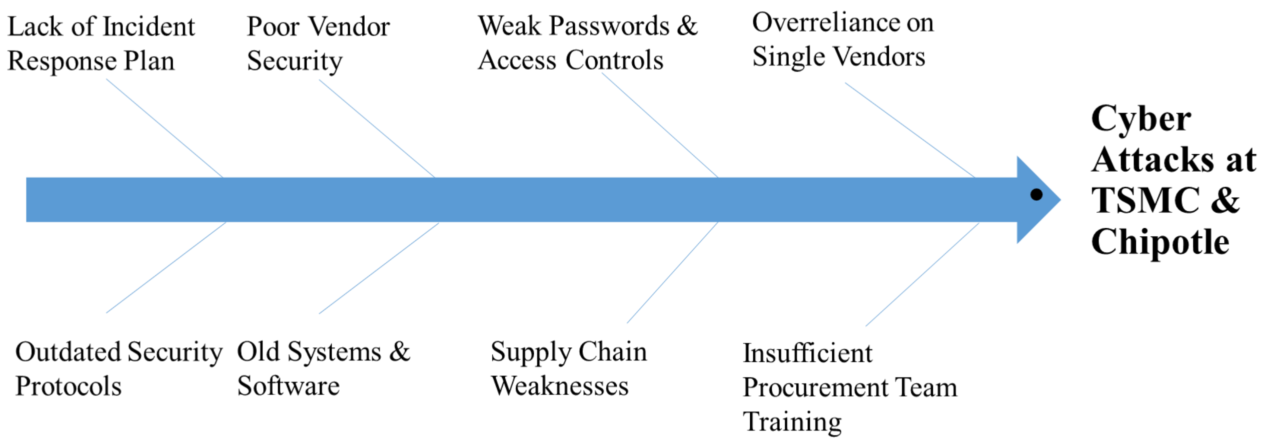
• Cybersecurity Challenges at TSMC

Taiwan Semiconductor Manufacturing Company (TSMC), on the other hand, struggles to secure its production systems and internal networks. A significant breach occurred when malware entered its manufacturing network via new equipment installation, causing production delays and financial losses. TSMC must enhance cybersecurity measures to prevent future incidents, maintain operational continuity, and protect its supply chain from external vulnerabilities.

By investigating these cases, this study aims to uncover critical insights into the vulnerabilities organizations face, particularly within their procurement and purchasing teams, and explore practical measures to enhance cybersecurity resilience in an increasingly interconnected world. The analysis highlights how procurement-related factors, such as insufficient vendor security assessments and inadequate scrutiny of supplier practices, contributed to the breaches at Chipotle and TSMC. The study also examines the impacts of these procurement vulnerabilities, including compromised systems, operational disruptions, and financial losses.

Furthermore, the paper explores actionable recommendations for procurement and purchasing teams to strengthen cybersecurity, including implementing stricter vendor evaluations, requiring cybersecurity compliance in supplier contracts, and adopting robust monitoring of supplierprovided systems. By addressing these procurement-specific factors, the study provides a comprehensive view of the causes, impacts, and strategies necessary to mitigate risks and strengthen cybersecurity frameworks across supply chains.

4. Fishbone Diagram Analysis: Factors Contributing to the Main Cybersecurity Problem


Lack of Incident Response Plan
Poor Vendor Security
Weak Passwords & Access Controls
Overreliance on Single Vendors
Cyber Attacks at TSMC & Chipotle
Outdated Security Protocols
Old Systems & Software
Supply Chain Weaknesses
Insufficient Procurement Team Training

- ## Lack of Incident Response Plan

The absence of a robust incident response plan specific to procurement activities played a crucial role in the cybersecurity breaches at both Chipotle and TSMC. At Chipotle, procurement teams failed to ensure that third-party vendors had established protocols for handling cyber threats, which delayed the detection of malware infiltrating its point-of-sale (POS) systems. Similarly, TSMC's procurement processes lacked clear criteria for assessing vendors' ability to respond to cyber incidents, contributing to the virus outbreak that disrupted production. These cases underscore the importance of procurement teams actively incorporating incident response readiness into vendor selection and management processes.

- ## Poor Vendor Security

The breaches at Chipotle and TSMC were significantly influenced by insufficient security oversight in vendor relationships. Chipotle’s procurement team relied on third-party vendors for POS systems without implementing stringent security requirements or regular vendor audits. This oversight allowed malware to exploit vulnerabilities in vendor-managed systems. At TSMC, procurement teams did not enforce comprehensive cybersecurity checks during the acquisition of third-party equipment, resulting in the introduction of a virus during installation.

Procurement teams must prioritize vendor security by integrating cybersecurity standards and monitoring compliance to mitigate such risks.

- Weak Passwords and Access Controls

Procurement teams at both companies played a role in perpetuating weak authentication practices within vendor systems. At Chipotle, the procurement team did not ensure vendors adhered to stringent password policies, enabling attackers to easily access POS systems and compromise customer data. Similarly, TSMC's procurement team failed to mandate robust access controls for third-party equipment and personnel, allowing the virus to spread. Incorporating access control requirements into procurement contracts and agreements could have mitigated these vulnerabilities.

- Supply Chain Weakness

Chipotle’s reliance on external payment system providers and TSMC’s dependence on third-party equipment suppliers demonstrated how procurement teams' decisions can introduce cybersecurity vulnerabilities. Chipotle’s procurement team did not perform thorough security assessments of payment system vendors, exposing the company to malware infiltration. Similarly, TSMC's procurement team’s inadequate oversight of equipment suppliers allowed a virus to disrupt production, directly affecting operations and cascading to partners like KLA Corp. Stronger procurement policies for evaluating supplier cybersecurity readiness would help address such weaknesses.

- Old Systems and Software

The use of outdated systems and software by suppliers highlighted lapses in procurement practices at both companies. Chipotle’s procurement team failed to mandate regular updates and security patches for vendor-managed POS systems, creating vulnerabilities that malware exploited. At TSMC, procurement teams did not establish clear upgrade requirements for production tools acquired from third-party vendors, leaving them vulnerable to sophisticated attacks. Procurement teams must integrate technology lifecycle management and upgrade requirements into vendor agreements to mitigate these risks.

- Outdated Security Protocols

Procurement teams contributed to outdated security protocols by not enforcing updated standards with vendors. At Chipotle, vendors managing POS systems adhered to outdated protocols, which were incapable of detecting modern threats, while TSMC’s suppliers lacked contemporary protections, enabling the virus to spread. Procurement teams should ensure all vendor systems meet updated security benchmarks as a condition for ongoing collaboration, reducing exposure to emerging threats.

- ### Overreliance on Single Vendors

Over-dependence on specific vendors can create single points of failure. At Chipotle, relying heavily on a single payment system provider magnified the impact of the breach. For TSMC, a similar reliance on a single equipment supplier may have exacerbated the spread of malware across its production systems.

- ### Insufficient Procurement Team Training

Procurement teams may have lacked adequate training in evaluating cybersecurity risks. At Chipotle, this could mean failing to recognize the importance of vendor security certifications, while at TSMC, it might have involved overlooking the cybersecurity implications of third-party equipment integration.

5. Quantitative Analysis

- ### Chipotle Mexican Grill

Industry: Quick-Service Restaurant (QSR)

Key Operations: Chipotle operates over 2,250 restaurants across North America, offering fast-casual Mexican-inspired cuisine. Its operations depend heavily on supply chain networks for sourcing ingredients (e.g., beef, chicken, lettuce, etc.), third-party payment processors for POS systems, and digital ordering systems.

Supply Chain Network Map:

- **Primary Suppliers:** Niman Ranch supplies sustainably raised meats, which are a core ingredient for Chipotle's menu, packaging suppliers, and transportation providers for food and goods distribution.
- **Secondary Suppliers:** External payment processors (e.g., Visa, Mastercard, and third-party vendors that manage POS systems), Oracle provides database and software solutions for operations, supply chain management, and analytics, while Interpublic Group delivers marketing and advertising services to boost brand awareness and customer engagement and delivery services

Cybersecurity Breach (2017): In April 2017, Chipotle's POS systems were compromised by malware. Hackers gained unauthorized access to the card payment data of customers, including credit card numbers, expiration dates, and security codes. The breach affected over 2,250 locations and was eventually discovered and mitigated.

SEC Reporting: Chipotle disclosed the breach in its SEC filings, emphasizing the steps taken to resolve the incident, including removing the malware and enhancing security protocols.

Supply Chain Risk: The breach occurred due to vulnerabilities in third-party managed POS systems, indicating that Chipotle's reliance on external suppliers for payment systems exposed it to cyber risks.

Chipotle's Risk Exposure: The quantitative risk estimation for Chipotle's supply chain considers the frequency of cyber incidents in the retail sector and the financial impact of such breaches. By combining these factors, a risk score is calculated as the product of incident frequency and potential financial impact. For example, with a moderate incident frequency as 2 (moderate frequency in retail sector) and an estimated breach cost of $20 million (estimated based on industry breach costs), the potential risk exposure is $40 million. The risk score suggests a moderate potential exposure of **$40 million**, highlighting the importance of strengthening cybersecurity measures for external service providers.

- ## TSMC (Taiwan Semiconductor Manufacturing Company)

Industry: Semiconductor Manufacturing

Key Operations: TSMC is a global leader in semiconductor fabrication, providing chips for major tech companies like Apple, Nvidia, and Qualcomm. Its operations are centered on large-scale manufacturing in Taiwan and include extensive global supply chains for raw materials, equipment, and customer products.

Supply Chain Network Map:

  - **Primary Suppliers:** KLA Corp provides quality control and yield management solutions, ASML supplies lithography equipment essential for chip fabrication, and SUMCO supplies silicon wafers for chip manufacturing.
  - **Secondary Suppliers:** DuPont provides materials like photoresists for semiconductor production, while Cadence supplies EDA software for chip design.

Cybersecurity Breach (2018): TSMC suffered a significant cyber-attack in August 2018 when malicious software (a virus) was introduced during the installation of a new equipment tool. The malware disrupted TSMC's production, leading to a financial loss of approximately $85 million in shipment delays.

SEC Reporting: In TSMC's SEC filings, they reported the virus incident, detailing how the malware spread through the network and caused significant operational disruptions. They also outlined corrective actions taken, such as enhancing firewall protections and implementing automated system checks for future installations.

Supply Chain Risk: The virus was introduced by a third-party supplier who installed compromised equipment. This incident highlights the significant supply chain risks that TSMC faces from external vendors.

TSMC's Risk Exposure: TSMC's reliance on third-party equipment suppliers introduces risks if malicious software or viruses are introduced through these vendors. In the 2018 breach, TSMC lost significant revenue and incurred high operational recovery costs due to the virus's impact on its production line. TSMC's supply chain risk is also significant due to its reliance on third-party equipment suppliers. The risk score of $85 million demonstrates the critical need for enhanced supplier security protocols and proactive monitoring of equipment installations.

6. Risk Mitigation Strategies for Supply Chain Cybersecurity

❖ Proactive Vendor Security Assessments

In procurement, vulnerabilities often arise from third-party vendors, which can introduce risks into the supply chain. Regular security assessments help ensure that vendors meet robust cybersecurity standards, reducing the chance of an attack originating from the supply side. For instance, Chipotle's breach stemmed from a third-party vendor's point-of-sale system, highlighting the risk of vendor-managed systems. By proactively identifying vulnerabilities, procurement teams can ensure that potential vendors have sufficient security measures in place, thereby minimizing the chances of a breach impacting the organization's sensitive data or operations.

Pros:

- Identifies vulnerabilities in vendor security before incidents occur, reducing the likelihood of breaches.
- Builds stronger, more transparent relationships with suppliers, establishing clear security expectations.
- Allows procurement teams to make informed decisions based on the security posture of potential vendors.

Cons:

- Time-consuming and resource-intensive to audit all suppliers regularly, especially for large or global supply chains.
- Some vendors may perceive the security assessments as intrusive, which could damage relationships or cause delays in negotiations.

❖ Implementing Real-Time Monitoring Systems in Vendor Networks

Procurement teams depend on the timely and secure delivery of goods and services from vendors, making it essential to monitor vendor networks for potential threats. Real-time monitoring of vendor systems can help detect security issues before they escalate into major breaches. For example, Chipotle's breach occurred due to delayed malware detection, while TSMC's virus outbreak spread due to a slow response. By monitoring vendor networks in real-time, procurement can proactively detect anomalies in activity, such as unauthorized access or malware activity, which could help contain threats before they affect supply chain operations or sensitive data.

Pros:

- Immediate detection of unusual or malicious activities within vendor networks, enabling quicker response to mitigate damage.
- Improves overall supply chain security by ensuring continuous visibility into vendors' security systems.
- Facilitates proactive management of vendor risks, especially in real-time data exchanges and transactions.

Cons:

- High initial costs for the implementation and maintenance of monitoring systems.
- Risk of false positives that may lead to unnecessary disruptions in supply chain operations or vendor relationships.

❖ Incident Response Planning with Vendors

A well-defined incident response plan is essential for swiftly addressing cyber incidents and minimizing the impact on supply chain operations. Procurement teams should ensure that vendors are part of the incident response strategy, with clear protocols to follow during an attack. The lack of predefined response strategies in Chipotle's and TSMC's cases led to prolonged disruptions. Having an incident response plan ensures that when a breach occurs, all stakeholders, including suppliers, can quickly and efficiently contain the issue, reducing downtime and limiting financial losses, as well as ensuring business continuity within the supply chain.

Pros:

- Reduces downtime and operational disruptions caused by cyberattacks, ensuring continuity in supply chain operations.

- Helps minimize the financial and reputational damage from incidents by allowing for a faster recovery.
- Ensures coordination with vendors during a cyber incident, improving overall crisis management.

Cons:

- Requires regular updates and testing to ensure the effectiveness of the incident response plans.
- Must involve all key stakeholders, including vendors and procurement teams, which can be difficult to manage if not properly coordinated.

❖ Employee and Supplier Cybersecurity Training

Cybersecurity breaches often stem from human error, making training an essential component of risk mitigation. Procurement teams should regularly train both internal employees and suppliers on cybersecurity best practices. For instance, Chipotle's breach was partly caused by weak password management, while TSMC's virus outbreak was linked to inadequate cybersecurity awareness during equipment installation. Regular training ensures that employees and suppliers understand the latest threats, such as phishing or insecure password practices, and can recognize vulnerabilities before they are exploited. Training programs are an effective way to address human error, which is a major cause of cybersecurity incidents.

Pros:

- Increases awareness and improves overall cybersecurity practices within the organization and across the supply chain.
- Cost-effective compared to other technical implementations.
- Reduces the chances of human error leading to breaches, such as weak passwords or mishandling sensitive data.

Cons:

- Requires ongoing training and updates to remain effective against new and evolving threats.
- May face resistance from employees or suppliers, particularly if the training is perceived as burdensome or unnecessary.

❖ Continuous Risk Assessment and Security Audits

Cyber threats evolve rapidly, and procurement teams must continuously assess the security posture of both internal systems and external vendors. Regular risk assessments help identify weaknesses before they can be exploited. Chipotle's outdated POS systems and TSMC's reliance on legacy software left both companies vulnerable to attacks. By conducting ongoing risk assessments and security audits, procurement teams can detect and address security gaps that could jeopardize sensitive data or disrupt supply chain operations. Continuous evaluation ensures that the organization adapts to emerging threats, maintaining a strong security posture and reducing the long-term risk of breaches.

Pros:

- Ensures that procurement decisions are informed by up-to-date risk assessments, helping to mitigate long-term vulnerabilities.
- Allows for continuous improvement in security measures and strategies to address emerging threats.
- Enhances resilience of the supply chain by identifying and addressing risks before they are exploited.

Cons:

- Requires specialized cybersecurity expertise, which can increase operational costs.
- May divert attention and resources away from other critical procurement activities, such as supplier relationship management.

❖ Vendor Risk Management Framework

A structured framework for managing vendor risks is vital for procurement teams to ensure that third-party vendors follow rigorous cybersecurity protocols. A comprehensive vendor risk management framework includes vendor assessments, contract clauses on security standards, and continuous monitoring of vendor activities. This approach ensures that cybersecurity is integrated into the procurement process from the beginning, minimizing risks associated with third-party vendors. The framework helps procurement teams evaluate vendors based on their security practices, ensuring that only those with adequate cybersecurity controls are chosen, thus reducing the risk of breaches originating from weak vendor security.

Pros:

- Provides a clear, standardized process for managing vendor risks across all stages of the procurement lifecycle.
- Facilitates better decision-making when selecting and managing vendors, ensuring that cybersecurity considerations are integrated into procurement decisions.
- Helps mitigate risks from vendors who may not have strong cybersecurity practices**.**

Cons:

- Implementing a comprehensive vendor risk management framework can be time-consuming and costly, especially for large organizations with many suppliers.
- Requires ongoing oversight and regular updates to ensure the framework remains relevant as new risks emerge.

❖ Strengthening Cybersecurity Contractual Clauses

Including cybersecurity-specific clauses in contracts with vendors ensures that they are legally obligated to meet certain security standards, such as encryption, data protection, and incident response protocols. Procurement teams play a key role in negotiating these clauses to ensure that vendors are held accountable for maintaining robust cybersecurity practices. These contractual clauses help mitigate risks by setting clear expectations for security and providing legal leverage to ensure compliance. By embedding these clauses into procurement contracts, organizations can protect themselves from third-party vulnerabilities, minimizing the risk of data breaches or operational disruptions originating from weak vendor security.

Pros:

- Provides legal and contractual leverage to enforce cybersecurity standards among vendors.
- Reduces the likelihood of vendor-related breaches by setting clear expectations.
- Facilitates greater accountability among vendors for maintaining high cybersecurity standards.

Cons:

- Vendors may resist the inclusion of stringent cybersecurity clauses, potentially delaying negotiations or resulting in higher costs.
- Enforcing these clauses may require additional resources, such as regular audits or compliance checks, to ensure vendors are adhering to contractual obligations.

7. Metrics table for recommendations

Metric	**Description**	**Success Indicator**	**Failure Indicator**
Vendor Compliance Rate	Percentage of third-party vendors meeting security requirements.	High compliance rate indicates effective vendor security assessments and strong risk management.	Low compliance rate suggests ineffective vendor evaluation or weak enforcement of security standards.

Incident Detection Time	Average time taken to detect a cyber incident.	Short detection time shows effective real-time monitoring systems identifying threats quickly.	Long detection time indicates inadequate monitoring systems or insufficient detection capabilities.
Response Time to Cyber Incidents	Average time taken to contain and resolve a cybersecurity incident.	Quick response time indicates an actionable and efficient incident response plan.	Delayed response time reflects poor incident response planning or lack of preparedness.
Employee and Supplier Security Awareness	Percentage of employees and suppliers completing cybersecurity training.	High completion rate and positive assessment results demonstrate strong cybersecurity awareness.	Low participation or poor assessment scores indicate gaps in training effectiveness or engagement.
Audit and Risk Assessment Outcomes	Number of security vulnerabilities identified during audits/assessments.	Reduction in vulnerabilities over time shows active efforts to improve security posture.	High or unchanged number of vulnerabilities indicates inadequate risk assessments or failure to address weaknesses.

8. Recommendations

Recommendations for Chipotle

1. **Proactive Vendor Security Assessments**
   Conducting regular security assessments of third-party vendors, such as payment processors and POS system providers, ensures they adhere to industry cybersecurity standards. This proactive measure reduces the likelihood of external threats entering the organization through vendor-managed systems, similar to the breach Chipotle experienced in 2017.

2. **Implement Real-Time Monitoring Systems**
   By implementing real-time monitoring for payment systems and customer data, Chipotle can detect suspicious activity and potential breaches immediately. Early detection allows

for a quicker response to mitigate any damage, helping to protect sensitive customer information from being compromised.

3. **Strengthen Incident Response Planning**
   Developing a robust, clear, and actionable incident response plan is essential for Chipotle to quickly respond to and contain cyber threats. A predefined response plan ensures that when a breach is detected, the company can act swiftly, minimizing damage to customer data, operations, and its reputation.

4. **Regular Employee and Supplier Cybersecurity Training**
   Educating employees and suppliers on cybersecurity best practices, such as recognizing phishing attempts and implementing strong password policies, can significantly reduce human error. Training helps create a culture of security awareness that empowers all stakeholders to play an active role in safeguarding sensitive data.

5. **Continuous Risk Assessments and Security Audits**
   Ongoing risk assessments and security audits help identify and address emerging vulnerabilities in Chipotle's systems and supply chain. Regular evaluations ensure that the company's technology stays up-to-date with evolving threats, reducing the risk of successful cyber-attacks.

Recommendations for TSMC

1. **Proactive Vendor Security Assessments**
   TSMC should assess its third-party suppliers, especially those providing critical production equipment, to ensure that their cybersecurity practices meet necessary standards. By addressing potential vulnerabilities in the supply chain, TSMC can prevent the introduction of cyber threats that could disrupt production and operations.

2. **Implement Real-Time Monitoring Systems**
   Real-time monitoring systems deployed across TSMC's production environments can provide early warnings of cyber threats. Continuous surveillance allows for swift identification of abnormal activities, enabling the company to take action before a cyber incident escalates into a major disruption.

3. **Strengthen Incident Response Planning**
   A well-defined incident response plan ensures TSMC can quickly and efficiently manage any cyberattack or virus outbreak. The ability to swiftly contain and recover from incidents limits production downtime, reduces financial losses, and prevents reputational damage.

4. **Regular Employee and Supplier Cybersecurity Training**
   Providing ongoing cybersecurity training for TSMC's employees and suppliers helps prevent the types of errors that led to the virus outbreak. Knowledgeable staff and

suppliers are less likely to overlook vulnerabilities or mishandle sensitive data during equipment installations and operations.

5. **Continuous Risk Assessments and Security Audits**
   TSMC should perform continuous risk assessments and security audits on its internal systems and vendor tools. These ongoing evaluations help detect outdated software, hardware vulnerabilities, or gaps in the security infrastructure, ensuring that TSMC's defenses remain robust against emerging cyber threats.

6. **Strengthen Cybersecurity Contractual Clauses with Vendors**
   Including strong cybersecurity clauses in contracts with suppliers can ensure that vendors maintain a high standard of security. This approach guarantees that any third-party equipment or software used by TSMC is secure and aligns with the company's cybersecurity requirements, preventing potential risks from entering the supply chain.

9. Conclusion

In conclusion, the 2017 Chipotle cyberattack highlighted major vulnerabilities in the company's cybersecurity practices, especially in relation to third-party vendor security, incident response, and system monitoring. The breach, which lasted over 20 days, exposed critical weaknesses in Chipotle's ability to respond swiftly and effectively to cyber threats, with inadequate monitoring of systems such as point-of-sale (POS) and payment gateways. To prevent similar incidents in the future, Chipotle's procurement and purchasing teams must prioritize proactive vendor security assessments, ensuring that third-party suppliers adhere to stringent cybersecurity standards. Additionally, real-time monitoring systems should be integrated into procurement processes to track and detect any anomalies across payment and supply chain systems. Strengthening incident response plans and ensuring regular cybersecurity training for both employees and suppliers will equip the team with the knowledge and tools to act swiftly in the event of a breach. Lastly, continuous security audits and risk assessments should be a routine part of the procurement process to address emerging threats and enhance overall supply chain security. By addressing these areas, Chipotle's procurement and purchasing teams can help improve the company's cybersecurity posture, protect sensitive customer data, and mitigate future risks in its supply chain and operations.

10. References

https://ir.chipotle.com/news-releases?item=122402

https://www.sec.gov/Archives/edgar/data/1058090/000105809018000018/cmg-20171231x10k.htm

https://pr.tsmc.com/english/news/1969

https://www.reuters.com/article/technology/apple-chip-supplier-tsmc-resumes-production-after-wannacry-attack-idUSKBN1KR0B8/

https://www.sec.gov/Archives/edgar/data/1046179/000119312519108390/d665387d20f.htm

https://ir.kla.com/financial-information/annual-reports

https://d1io3yog0oux5.cloudfront.net/_b625e77f311c923131ab618bd8bea36b/klatencor/db/1157/9983/annual_report/2019_AR.pdf