Best practices in supplier relationship management and response when supply is disrupted by cyber attack: An incident response framework

Received: 1st April, 2023

Cyrus Green

Vice President, Business Resilience, T. Rowe Price, USA

Cyrus Green

Cyrus Green *is a Vice President at T. Rowe Price, where he is a senior manager on the Business Resilience Team. As a certified business continuity professional, Cyrus plays a pivotal role in managing and overseeing the resiliency efforts for global distribution, global marketing and global product divisions within T. Rowe Price. He leads the company's proactive preparations to effectively mitigate, adapt, and respond to disruptive situations, ensuring the continuous operation of critical business functions while prioritising the safety of staff, guests, property and brand equity. Cyrus holds a doctor of business administration degree from the University of Maryland Global Campus, where his research focused on supplier resiliency. As a scholar-practitioner, he actively contributes to industry events and publications, sharing his insights and expertise on various topics related to resilience and organisation supplier management.*

Enterprise Risk Group,
T. Rowe Price,
4515 Painters Mills Road,
OM-1310,
Owings Mills,
MD 21117-4903,
USA

E-mail: cyrus.green@troweprice.com

Journal of Business Continuity & Emergency Planning
Vol. 17, No. 1, pp. 6–15

1749–9216

Abstract

This paper explores the growing dependency of organisations on suppliers and the importance of supplier relationship management (SRM) in achieving sustainable competitive advantage. It highlights the various reasons organisations engage with suppliers, including accessing specialised expertise, cost savings, flexibility, risk mitigation and improved quality. The paper emphasises the need for organisations to adopt best practices in SRM to enhance their resilience to disruptions, particularly those caused by cyber attacks. It introduces a threat assessment process for organisations to evaluate the potential impact of supplier disruptions and proposes strategies for improving resilience through collaboration with suppliers. The article also discusses the significance of data sharing between organisations and suppliers, outlining different channels and methods for secure data exchange. It addresses the risks associated with data sharing, such as breaches, intellectual property theft, compliance violations and loss of control. Additionally, the article examines the impacts of supplier disruptions on organisations and emphasises the importance of establishing clear guidelines and policies for data sharing. It concludes by presenting a threat assessment process for supplier disruptions due to cyber attacks, including identifying critical suppliers, conducting risk assessments, analysing findings, developing mitigation strategies, implementing strategies and conducting ongoing monitoring.

Keywords: supplier disruption, supplier relationship management, supplier resilience, extreme disruption, cyber attack

INTRODUCTION

Suppliers and procurement are vital drivers of sustainable competitive advantage for organisations. Organisations utilise suppliers for various reasons, including access

to specialised expertise, cost savings, flexibility, risk mitigation and improved quality. Suppliers often have specialised expertise and knowledge that organisations may need in-house. Organisations that work with suppliers can access this expertise and benefit from their knowledge and experience. Organisations that outsource certain functions to suppliers can often save money, as suppliers can often provide economies of scale and access to lower-cost raw materials or labour, resulting in cost savings for the organisation. Organisations that work with suppliers can benefit from greater flexibility in terms of their capacity and capabilities. For example, organisations that outsource certain functions can scale their operations up or down more efficiently, and adjust their product offerings more quickly in response to changes in the market. Suppliers can often provide goods and services of a higher quality than organisations can produce in-house. If one supplier cannot provide goods or services, the organisation can turn to another supplier to fill the gap. Organisations diversifying their supplier base can reduce their risk of supply chain disruptions.

This article describes the best practices in supplier relationship management (SRM) that organisations should strive to have in place before a disruptive event. Organisations and suppliers utilise and share data to perform critical products and services.[1] When suppliers inevitably experience disruptions to their products and services, this impacts their clients. Organisations thus require more complex solutions and collaboration in order to become more resilient. Amid uncertainty, global warming, tariffs and trade wars, global organisations must be equipped to manage complex global suppliers effectively.[2] This article introduces an initial threat assessment process for organisations to determine whether supplier disruption will impact the delivery of current or future business products or services. The literature proposes several strategies organisations can use in conjunction with their suppliers to improve their resilience to disruption by cyber attack.

ORGANISATIONS UTILISING SUPPLIER RELATIONSHIP MANAGEMENT BEST PRACTICES

The effective management of suppliers is important in order to diminish risk and uncertainty and optimise products or services in order to satisfy customers and ensure profits.[3] 'Supplier relationship management' or 'supplier management' (this article uses the terms interchangeably) is a comprehensive approach to managing an organisation's interactions with the third-party organisations that supply them with products and services.[4]

The concept of SRM was coined in the late 1980s and is defined as 'the process of planning and managing all relationships with vendors that supply any products or services to a business'.[5] SRM involves managing the relationships and interactions between an organisation and its suppliers to maximise value and minimise risk. Organisations can employ SRM best practices to optimise the supplier selection process, establish clear communication channels, collaborate with suppliers, monitor supplier performance, build strong relationships, manage risk and continuously improve. The supplier selection process should be rigorous and ensure that suppliers meet the organisation's requirements for quality, cost and reliability.

Organisations should also consider the supplier's financial stability, reputation and capacity to deliver on time. Clear communication channels are essential to effective SRM. Organisations should establish regular communication with suppliers to discuss expectations, performance and any issues. Clear communication also

helps to build trust and understanding between parties. Organisations should work closely with suppliers to identify opportunities for collaboration and innovation. Collaboration can involve joint problem-solving, sharing best practices and exploring ways to improve processes and reduce costs.

Organisations should regularly monitor supplier performance against key performance indicators to ensure they meet expectations. Monitoring suppliers can involve tracking delivery times, quality and cost performance. Building solid relationships with suppliers is critical to effective SRM. SRM can involve recognising suppliers' contributions, providing feedback and support, and developing mutual respect and trust.

Organisations should assess and manage the risk associated with suppliers. Risk management can involve identifying potential supply chain disruptions, developing contingency plans and establishing performance improvement plans when necessary. Organisations should continuously review and improve their SRM processes to ensure they are practical and efficient. SRM can involve analysing supplier performance data, soliciting supplier feedback and incorporating lessons learned into future supplier management practices.

An important aspect in SRM is for organisations to implement a tiering process. A tiering process is a method of ranking suppliers based on various criteria, including quality, delivery, price and reliability. This process involves categorising suppliers into different tiers based on their performance and importance to the organisation.

Tier 1 comprises strategic suppliers that are critical to the organisation's success. They typically supply key components or raw materials that are essential to the organisation's operations. As we have moved from the industrial age into the information age, the critical raw material of today is data. These suppliers are often long-term partners and have a high level of integration with the organisation's processes.

Tier 2 includes preferred suppliers that are suppliers that are important to the organisation's success, but are not as critical as Tier 1 suppliers. They may supply non-critical components or materials that can be sourced from multiple suppliers. These suppliers may have a strong track record of quality and reliability and may offer competitive pricing.

Tier 3 includes approved suppliers who have met the organisation's minimum requirements for quality, delivery and reliability. They may supply non-critical components or materials that are readily available from multiple sources. These suppliers may offer competitive pricing but may not have a strong track record of quality and reliability.

Tier 4 includes basic suppliers that meet the organisation's minimum requirements but are neither preferred nor approved suppliers. They may supply non-critical components or materials that are readily available from multiple sources. These suppliers may offer competitive pricing but may not have a strong track record of quality and reliability.

It is important to note that the tier process is not a static ranking and should be regularly reviewed and updated based on supplier performance and changes in the organisation's needs and priorities. The process should also allow for new suppliers to be added or existing suppliers to move up or down the tiers based on their performance.

ORGANISATIONS AND SUPPLIERS SHARING DATA

Data sharing between organisations and suppliers can occur through various

channels and methods, depending on the nature of the data, the level of collaboration and security and confidentiality requirements.[6] Organisations and suppliers share data through Electronic Data Interchange (EDI), application programming interfaces (APIs), cloud-based collaboration tools, secure File Transfer Protocol (SFTP) and web-based portals. EDI involves the exchange of business documents, such as purchase orders, invoices and shipping notices, in a standardised electronic format. EDI allows for the seamless and automated transfer of data between organisations and suppliers, reducing errors and improving efficiency. APIs are sets of protocols and tools for building software applications. APIs can enable data sharing between organisations and suppliers by allowing applications to communicate and exchange data in a secure and standardised manner. Cloud-based collaboration tools like SharePoint, Google Drive and Dropbox can be used to share documents, files and other data between organisations and suppliers. These tools enable real-time collaboration, version control and secure access to shared data. SFTP is a secure protocol for transferring files over the internet, and can be used to share large files, such as product specifications or designs, between organisations and suppliers in a secure and encrypted manner. Web-based portals can provide suppliers access to relevant data and information, such as production schedules, inventory levels and quality metrics. These portals can be customised to the needs of each supplier and can provide real-time access to critical data.

Regardless of the method, the sharing of data between organisations and suppliers must be done securely and with appropriate access control and data protection levels. To ensure that sensitive information is not compromised, it is essential to establish clear guidelines and policies for data sharing, including data ownership, security and confidentiality.

ORGANISATIONS IMPACTED BY SUPPLIER DISRUPTION

Sharing data between organisations and suppliers can bring many benefits, such as improving collaboration, increasing efficiency and reducing costs. However, it also comes with risks, such as data breaches, intellectual property theft, compliance violations, misuse of data and loss of control.

Sharing data with suppliers increases the risk of data breaches, as suppliers may have different security measures than the organisation. When sensitive information, such as financial or customer information, is compromised, this can lead to reputational damage, legal liability and financial losses.[7] Sharing sensitive information with suppliers, such as product designs or trade secrets, increases the risk of intellectual property theft. If suppliers use this information for their benefit or share it with competitors, it can harm the organisation's competitive advantage and lead to lost revenue. Sharing data with suppliers may also increase the risk of compliance violations, such as data privacy or industry-specific regulations. When suppliers fail to comply with these regulations, this can lead to legal penalties and reputational damage. Sharing data with suppliers may also increase the risk of data misuse, such as using data for purposes outside the agreed scope or sharing data with unauthorised third parties. Sharing data with suppliers can also lead to losing control over the data, as suppliers may use the data in a way that deviates from the organisation's goals or values.

Organisations should establish clear guidelines and policies for data sharing to mitigate these risks, including data ownership, security and confidentiality.

Organisations should also conduct due diligence on suppliers to ensure they have appropriate security measures and comply with relevant regulations. Finally, organisations should monitor supplier compliance and performance to ensure they meet expectations and protect the organisation's data.

SUPPLIERS DISRUPTED BY CYBER ATTACK

A supplier disruption begins with a mistake or issue that results in a disturbance or interruption to a process that impacts a product or service intended for the end customer. Cyber attacks are a significant threat to organisations of all sizes and industries, and all indicators point to the problem escalating rapidly. A cyber attack on a supplier can significantly impact an organisation and its customers. The potential impacts include disruption of services, loss of customer data, financial losses, supply chain disruption and reputational damage.[8] A cyber attack can disrupt the supplier's services, leading to customer delays or downtime. Disruption can cause inconvenience, loss of productivity and even financial losses. If the cyber attack results in the loss or theft of customer data, the supplier, vendor or service provider may face legal and regulatory penalties and damage to their reputation. A cyber attack can also result in financial losses for the supplier, such as the cost of investigating and mitigating the attack, compensating affected customers and potentially losing business. If the supplier is part of a supply chain, a cyber attack could disrupt the entire chain, causing delays and financial losses for all parties involved. A cyber attack can damage the supplier's reputation, particularly if they are perceived as having inadequate security measures in place to protect their customers' data. The management challenges and consequences of supplier disruptions include but are not limited to impaired service or product outcomes, loss of productivity, revenue, customer loyalty, decreased competitive advantage and increased operating cost.

THE THREAT ASSESSMENT PROCESS FOR SUPPLIER DISRUPTION DUE TO CYBER ATTACK

Organisations rely on third-party suppliers to provide goods and services that are essential to their operations. The use of such suppliers, however, increases the organisation's potential exposure to cyber attacks, which can in turn lead to supply chain disruption, loss of data and reputational damage.[9] To manage the risk of supplier disruption due to cyber attack, organisations can implement a threat assessment process. The process entails identifying critical suppliers, conducting risk assessment and supplier security questionnaires (Tables 1 and 2), analysing the findings, developing mitigation strategies, implementing those mitigation strategies and conducting ongoing monitoring.

Organisations must identify the critical suppliers whose disruption could significantly impact their operations. These suppliers should be then prioritised for risk assessment. This assessment should include evaluating the supplier's security controls, such as firewalls, antivirus software and data backup processes. It should also evaluate the supplier's overall security posture, such as its security policies, procedures and incident response plan. Organisations can obtain such information by sending a security questionnaire to critical suppliers to gather more information about their security controls and practices.

After gathering information from the risk assessment and security questionnaire, the organisation should analyse the findings and identify potential vulnerabilities that could lead to a cyber attack and

Table 1: Supplier risk assessment questionnaire

Question	*Response*
Are policies and standards based on industry accepted standards and practices?	Yes or no
Do the information security policies contain statements concerning the organisation's definition of information security, objective and principles to guide all activities relating to information security?	Yes or no
Do owners review and update policies if significant changes occur in legal, business, organisational or technical conditions?	Yes or no
Have all information security policies and standards been reviewed in the last 12 months?	Yes or no
Does the organisation's board of directors or ownership require management to regularly demonstrate that the information security programme meets its intended objectives?	Yes or no
Are information security personnel responsible for the creation and review of information security policies?	Yes or no
Do information security personnel maintain professional security certifications?	Yes or no
Do information security personnel maintain contacts with information security special interest groups, specialist security forums or professional associations?	Yes or no
Do Information security personnel participate in continuing education programs (eg online training, webinars, seminars, etc)?	Yes or no
Use of firewall and VPN?	Yes, no or both
Use of encryption to protect sensitive data and messages?	Yes, no or both

Table 2: Supplier security assessment questionnaire

Question	*Descriptions*
What is the supplier's tier rating?	Tier 1, Tier 2, Tier 3 or Tier 4
What region(s) of the organisation are impacted?	North America, Europe, Middle East, Africa or Asia Pacific
What methods of connectivity does the supplier maintain with the organisation?	Electronic Data Interchange (EDI), application programming interfaces (APIs), cloud-based collaboration tools, Secure File Transfer Protocol (SFTP) or web-based portals.
What volume of organisation data does the supplier maintain that may have been exposed?	Number of records, year of earliest record, etc
What types of data does the supplier have access to?	Client data, associate data, board materials, internal budgets, supplier spend, internal policies & procedures, disclosed investment data or public data
What specific data types (ie client data or associate data)?	full or partial names, full or partial social security number or other governmental ID number, physical address or phone number, account number, credit card number, asset-type data (account balance, salary, etc), health-related data, racial or ethnic origin data, biometric data, political or religious beliefs/affiliations, sexual orientation
If this supplier fails to meet its obligations, do we have a regulatory violation?	Yes or no
Will the supplier provide products or services directly to clients?	Yes or no

supplier disruption. Where an organisation suspects that a critical supplier is vulnerable to a potentially disruptive cyber incident, it will invoke its supplier management team to communicate with the supplier relationship owners to review the supplier risk assessment questionnaires with the suppliers themselves.

Organisations can provide resources and support to their suppliers to improve their security posture or implement monitoring systems to detect and respond to potential cyber attacks. The organisation should develop mitigation strategies to address any vulnerabilities identified in the risk assessment. Such strategies could include requiring the supplier to improve its security controls, implementing monitoring systems to detect potential cyber attacks and creating a contingency plan in case of a disruption. The organisation should then work with the supplier to implement the mitigation strategies developed in the previous step.

The organisation should also continue monitoring its critical suppliers and their security controls to ensure they remain practical and up-to-date. Strategies could involve periodic risk assessments, security questionnaires or regular audits of the supplier's security controls. By following these steps, the organisation can identify and mitigate potential threats to critical suppliers and reduce the risk of cyber attacks leading to supplier disruption.

CYBER THREAT ASSESSMENT WORKING GROUP AND ORGANISATION INCIDENT RESPONSE

The result of an initial cyber threat assessment is to determine the incident risk level. The different sections of the assessment will inform the decision with respect to the breach fact pattern, organisation–supplier relationship and operational impact (Table 3). The breach fact pattern is often not fully known for weeks or months; the assessment may therefore default to a higher grade of risk until the full facts are known. The cyber threat assessment working group (Table 4) will partner with other stakeholders to assess the threat level using threat assessment criteria (Table 5) to determine the risk of the incident to the organisation's operations (ie low/medium/high), and initiate predetermined mitigative response actions identified for that threat assessment level, should it be is determined that a supplier has been impacted and data are at risk.

It is imperative to understand the supplier's role in servicing the organisation and the type and scope of data that the cyber incident might compromise.[10] Preliminary details of the incident must be acquired within 24 hours. For this reason, it is essential to have a direct line of contact with the supplier relationship manager or another responsible party at the affected supplier. It is also critical to record all available information about the incident in the organisation's incident management database tool as soon as possible.

If a threat is considered 'low', it may be decided to leave supplier relationship management to monitor the incident without further escalation. Should the fact pattern change, supplier management or supplier risk will adjust the threat assessment rating and implement/relax the core set of internal response measures. If, for example, a threat assessment identifies a threat as 'medium' or 'high', supplier management will invoke the organisation's incident response process to facilitate the response effort until resolution, and will convene the cyber threat assessment working group to ensure the appropriate resolution of the incident. Supplier management will update the cyber threat assessment working group on the situation and the response progress, and will start a

situation report to document the response to the incident. The situation report will detail corrective actions from the incident response, and ownership will be assigned accordingly.

The incident may emerge as 'medium 'or 'high' but later be downgraded to 'low' if facts pointing to a reduced risk are gathered. Once this occurs, supplier management will close the response effort and complete the final action steps to close the incident (eg gather any final documentation and append the organisation's incident management database tool record).

CONCLUSION

This article is intended to provide guidance and criteria for conducting an initial threat assessment regarding a cyber incident that impacts a supplier. Organisations are encouraged to partner with their

Table 3: Initial threat, fact pattern, supplier relationship and operational assessment

Initial threat assessment questionnaire	*Description*
Which supplier is compromised?	Identify the impacted supplier
What products and or services dos this cyber incident impact?	Identify with the business units what products or services are impacted by the cyber incident?
What type of attack/breach is it?	Ransomware, DDoS ransomware, phishing, other or unknown
Is the breach still active?	Yes, no or unknown
How long was the breach active before it was discovered?	Minutes, hours, days, weeks or months
What actions has the supplier taken to mitigate the attack?	Eliminated threat, quarantined environment, etc.
What is the known scope of the breach across the supplier's network?	Single system, multiple systems or most systems and infrastructure
Are the data locked or exfiltrated (stolen)?	Locked, stolen, both, unconfirmed or no data loss
If localised and currently contained, what is the probability the breach will escalate?	Not likely, possible, likely or unsure
What is public knowledge? Does this align with the information that the supplier is sharing?	News media, social media, etc.

Table 4: Cyber threat assessment working group

Cyber threat assessment working group	*Responsible, accountable, consulted or informed*
Reporting business unit engagement lead	Accountable
Supplier engagement manager	Responsible
Enterprise security	Consulted
Business continuity/resilience	Consulted
Supplier risk representative	Responsible
Business and operational risk	Informed
Technology risk	Informed
Corporate communications	Consulted
Privacy	Consulted

Table 5: Initial threat assessment incident risk criteria

Threat	*Descriptions*	*Examples*
Low	No personal data No confidential data No direct network access	No exposure
Medium	Potential exposure personal data Potential exposure confidential data Potential direct network access or sophisticated cyber attack	Contact information (name, phone number, address, e-mail, etc)
High	Confirm exposure personal data Confirm exposure confidential data Confirm direct network access or sophisticated cyber attack	Personal information (social security number, DOB, account number, biometrics, credentials, etc)

suppliers to analyse their resilience, assess their joint risk exposure, track supplier performance based on risk metrics, share forecasting and risk information with suppliers, build redundancy and flexibility in their supply chain networks (eg multiple manufacturing sites or suppliers) and develop business continuity plans or risk management systems with suppliers. By implementing these best practices, organisations can establish strong, mutually beneficial relationships with their suppliers, maximise value and minimise risk in their supplier ecosystem.

References

(1) Bowersox, D. J., Closs, D. J. and Stank, T .P. (2000) 'Ten mega-trends that will revolutionize supply chain logistics', *Journal of Business Logistics*, Vol. 21, No. 2, pp. 1–16.

(2) Attinasi, M. G., Balatti, M., Mancini, M. and Metelli, L. (2022) 'Supply chain disruptions and the effects on the global economy', *Economic Bulletin Boxes*, Vol. 8, available at: https://www.ecb.europa.eu//pub/economic-bulletin/focus/2022/html/ecb.ebbox202108_01~e8ceebe51f.en.html (accessed 23rd May, 2023).

(3) Green, C. L. (2022) 'Identifying supplier management best practices to sustain organization resilience: a systematic review', doctoral dissertation, University of Maryland University College.

(4) Mettler, T. and Rohner, P. (2009) 'Supplier relationship management: A case study in the context of health care', *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 4, No. 3, pp. 58–71.

(5) Dwyer, F. R., Schurr, P. H. and Oh, S. (1987) 'Developing buyer-seller relationships', *Journal of Marketing*, Vol. 51, No. 2, pp. 11–27.

(6) Smith, G. E., Watson, K. J., Baker, W. H. and Pokorski II, J. A. (2007) 'A critical balance: Collaboration and security in the IT-enabled supply chain', *International Journal of Production Research*, Vol. 45, No. 11, pp. 2595–2613.

(7) Brockett, P. L., Golden L. L. and Wolman, W. (2012) 'Enterprise Cyber Risk Management', in Emblemsvåg, J. -(ed.) 'Risk Management for the Future — Theory and Cases', IntechOpen, e-book available at: http://dx.doi.org/10.5772/1809, pp. 319–340.

(8) Beattie, J. and Shandrowski, M. (2021) 'Cyber-compromised data recovery: The more likely disaster recovery use case', *Journal of Business Continuity & Emergency Planning*, Vol. 15, No. 2, pp. 114–126.

(9) Ghadge, A., Weiß, M., Caldwell, N. D. and Wilding, R. (2020) 'Managing

cyber risk in supply chains: A review and research agenda', S*upply Chain Management: An International Journal*, Vol. 25, No. 2, pp. 223–240.

(10) Tallon, P .P. (2013) 'Corporate governance of big data: Perspectives on value, risk, and cost', *Computer*, Vol. 46, No. 6, pp. 32–38.