Greater Manchester | Greater Security | Greater Business

Cyber Foundry

Collaborative Cyber Security

Strength Through Shared Knowledge and Strategies

Audience: General **Reading Time: 5 Mins**

In today's digitally-driven era, cybersecurity is a priority for all businesses, regardless of size. Small and Medium Enterprises (SMEs) are particularly vulnerable, as they often lack the resources of larger companies to implement comprehensive cybersecurity measures. Yet, through collaboration, SMEs can overcome these challenges, effectively developing, and implementing a shared cybersecurity plan and protocol.

Why is there a need for SMEs to collaborate around cyber security? Cybercriminals are increasingly targeting SMEs, capitalising on their often-underdeveloped security infrastructures. A cybersecurity breach can have devastating consequences, potentially causing irreparable damage to a company's reputation, financial standing, and business continuity.

Collaboration can mitigate these risks, allowing SMEs to pool resources, share knowledge, and improve their overall cybersecurity stance. This approach enhances their capabilities to combat evolving cyber threats whilst increasing operational efficiencies.

The argument for cybersecurity collaboration amongst SMEs is rooted in three primary advantages: shared resources, collective intelligence, and heightened resilience.

Shared Resources: Cyber security infrastructure can be expensive, requiring investments in software, hardware, personnel, and training. By collaborating, SMEs can pool their resources to invest in advanced, shared cybersecurity solutions that might be cost-prohibitive for individual businesses. Collaborative arrangements may allow SMEs to leverage economies of scale, ensuring greater security coverage with reduced individual expenses.

Collective Intelligence: By working together, SMEs can tap into a broad network of insights, experiences, and expertise. Cyber threats are continually evolving, and keeping up can be a significant challenge for SMEs with limited resources. Collaborative partnerships allow for the exchange of threat intelligence, the sharing of best practices, and the joint development of cybersecurity strategies.

European Union
European Regional Development Fund
The Cyber Foundry project is part funded by the European Regional Development Fund

Lancaster University
MANCHESTER 1824 The University of Manchester
Manchester Metropolitan University
University of Salford MANCHESTER

Collective intelligence can enhance the ability of SMEs to anticipate, prevent, and respond to cyber threats.

Heightened Resilience: Cyber security collaboration can increase the resilience of SMEs in the face of cyber-attacks. Jointly developed incident response plans and shared recovery resources can expedite the restoration of normal operations following a cyber incident. In addition, collective lobbying power can influence policymakers and service providers to better cater to the cybersecurity needs of SMEs.

Steps for SMEs to Collaboratively Develop and Implement a Cybersecurity Plan

1. Establish a Collaborative Framework:
The first step would be to identify like-minded SMEs willing to collaborate on cybersecurity. This could be companies within the same industry or geographical region, or simply those that share similar digital structures or challenges. Establishing a cooperative agreement, detailing the responsibilities, expectations, and confidentiality clauses, provides a foundation for the collaborative endeavour.

Collaboration can mitigate these risks, allowing SMEs to pool resources, share knowledge, and improve their overall cybersecurity stance.

2. Share Knowledge and Best Practices:
Each SME brings unique experiences and insights to the table. By sharing knowledge and best practices, these enterprises can learn from each other's successes and failures, ultimately strengthening their collective cybersecurity protocols. This includes sharing information on potential threats, effective security measures, and lessons learned from past security incidents.

3. Regularly Conduct Threat Intelligence:
Threat intelligence involves gathering, analysing, and disseminating information about potential or current threats that could harm an organisation. Through collaboration, SMEs can pool resources to invest in threat intelligence services or jointly hire a cybersecurity expert. Shared threat intelligence allows participants to stay ahead of potential cyber threats, ensuring all partners are alerted to new risks.

4. Jointly Develop a Cybersecurity Plan:
Once the collaboration is in place and threat intelligence has been gathered, it is time to jointly develop a cybersecurity plan. This plan would outline prevention strategies, detection methods, response procedures, and recovery plans. A strong cybersecurity plan considers not just technical measures, but also human factors and business processes. It should be comprehensive yet flexible enough to accommodate the unique needs and capabilities of each participating SME.

5. Implement Cybersecurity Training:
SMEs can further maximise their collaborative efforts by organising joint cybersecurity training sessions for their employees. Regular training can help ensure that all employees are aware of potential cyber threats and know

how to respond appropriately. Cybersecurity is not just an IT concern - everyone has a role to play in keeping a company safe from cyber threats.

6. Monitor, Evaluate, and Adjust:
After implementing the cybersecurity plan, it becomes crucial to monitor its effectiveness continually. SMEs should jointly develop key performance indicators (KPIs) and metrics to measure the success of their cybersecurity efforts. Regular evaluations will help identify areas for improvement, enabling SMEs to adapt and evolve their cybersecurity strategies to address emerging threats effectively.

Potential Limitations of Cybersecurity Collaboration

Whilst collaboration offers significant benefits, it would be naïve to suggest that it does not come without certain challenges that SMEs must carefully consider.

Trust and Confidentiality Issues:
Sharing information about cybersecurity vulnerabilities and incidents requires a high level of trust between participating SMEs. There is a risk of sensitive information leaking or being misused. Additionally, collaborations may expose SMEs to new risks if partner organisations have poor cybersecurity practices. Therefore, it is crucial to establish strict confidentiality agreements and rigorous vetting processes.

Coordination Challenges:
Collaborating with other SMEs could potentially lead to coordination issues. Differences in organisational cultures, operational procedures, and communication styles can create friction. Successful collaboration requires clear, effective communication and a shared commitment to cybersecurity goals.
Legal and Regulatory Concerns

In certain areas, sharing specific types of information might be constrained by legal and regulatory requirements, particularly regarding privacy and data protection. Before establishing a collaborative agreement, SMEs should consult with legal experts to understand potential legal implications.

Resource Imbalance:
Whilst pooling resources has many advantages, it can also create complications. Differences in financial strength and cybersecurity maturity amongst SMEs can lead to imbalances in contribution and benefits. Ensuring fair contribution and equitable distribution can be challenging.

Navigating the Collaboration Landscape:
Despite these potential limitations, the advantages of cybersecurity collaboration are substantial. The key to a successful relationship is careful planning, stringent vetting of partners, clear communication, and constant monitoring and adjustment of the collaboration strategy. SMEs need not shy away from exploring collaborative opportunities but should do so in a manner that acknowledges, and plans for, the inherent challenges.

Collaborative cybersecurity is not a panacea but a tool. If used wisely, it can significantly enhance the cybersecurity posture of SMEs, fostering a safer and more secure digital environment for all.