The Path to Partnership:
Cyber Security in the Supply Chain

OT Cyber Security
Supply Chain

Expert Group

Introducing Admin Corp’s supply chain scenario

Purpose of this slide deck

This slide deck has been written to help the reader explore the dynamics in achieving good cyber security outcomes where client organisations use service providers to deliver solutions and services. It tells a story of a recommended procurement process and shows how cyber security responsibilities are shared and the different perspectives of customers and suppliers in how this is achieved.

Managing cyber security in the supply chain is a key concern of all organisations. Dependency on suppliers is more critical than it ever has been, and we continue to see cyber security attacks on the supply chain with impacts on their customers.

As a result, much work is being done internationally by government agencies, industry groups and standards bodies in developing relevant guidance and establishing regulations. It is therefore difficult to create a scenario which keeps up with all of these developments. Instead, we focus on what does not change - which is the dynamic of the relationship between customer and supplier and how a partnership approach is required. In the storyline, we give examples of the most commonly adopted standards used at present. Your circumstances, such as industry sector, may differ from these but the customer/supplier dynamics will remain the same and are the most important factors for success.

Introducing Admin Corp & Supply Corp

Admin Corp, a company providing essential services across the UK, is faced with a critical infrastructure challenge—the public switched telephone network (PSTN) is being switched off, and they need a modern IP-based network replace to their old dial-up systems. The new system will not only connect their control room with distributed operational technology (OT) sites but also upgrade their "man-down" wireless phones used by lone workers.

Admin Corp are regulated under the UK **Network and Information Systems (NIS) Regulations** and also have strict safety obligations.

The colours in the following dialogue highlight the relevant organisation.

Supply Corp

A system integration supplier of IT networking services who have expanded relatively quickly as a provider in a growing number of European countries. They have been very successful in running PSTN switchover projects for old dial-up building management systems, including physical security, alarms and lifts.

ACT 1 – Shortlisting Suppliers (RFI)

RFI

The first stage of the procurement process by Admin Corp is to create a first stage shortlist of potential suppliers who specialize in network integration. The procurement team started by developing an initial request for information (RFI) survey to the market which included some initial due diligence questionnaires on important topics such as compliance with environmental and anti bribery and corruption regulations, and included high level questions about information/cyber security which asked if a company held a certification under the ISO 27001 information security standard and/or certification against Cyber Essentials Plus.

The RFI is issued to a list of potential suppliers who specialize in network integration.

Supply Corp receive the RFI from Admin Corp. They submit a detailed response, highlighting their experience with PSTN switchovers and their capability to handle critical infrastructure projects across Europe.

Supply Corp makes it to the shortlist.

Admin Corp's cyber security team become aware of the procurement and discussed security questions which might be asked in the RFI. The security team cautioned that ISO 27001 certification will usually have limited scope applying to just part of a company's operations, often their head office. They proposed that a full risk assessment of the service to be delivered should drive the questions to be asked, although this may be difficult to do in an RFI. Eventually both teams agreed that this risk work should be done at the later RFP stage.

The security team cautioned that an assessment against ISO 27001 might be difficult for small companies and suggested that Cyber Essentials Plus also be considered. In addition they pointed procurement towards ISO/IEC 27036:2023 which covers approaches for supplier relationships/

Supply Corp are pleased to receive the RFI and are keen to respond. They do have an ISO 27001 certificate covering their UK office systems. They do not have any experience of the Cyber Essentials Plus process but decide that they would be prepared to go through this should they win the contract.

ACT 2a – Risk Assessment

The Admin Corp Cyber Security Team run a risk assessment workshop with the key stakeholders from their company who have knowledge of the technical and business context of the systems that will use the new network. This includes business leadership, IT, OT Engineering, Legal and Health and Safety. The workshop captures:

1. **Risk Impacts:**
    - Connections to sites could become unavailable, this could impact production and logistics and also have a safety concerns because of the ‘man down’ use of telephony.
    - Integrity and reliability/continuity of the OT systems could be impacted if their software or systems were interfered with.
    - If data was accessed it could be leaked outside the company – for much information this is not important but personal information (including health records) has data protection obligations, and pricing and production information is commercially sensitive**.**
2. **How Risks Might Arise:**
    - Risk in security of system design and the design, build and maintenance of devices and software used in the system.
    - Security of network connectivity/logical access by supplier to Admin Corp networks.
    - Security of physical access to systems by supplier staff on site visits.
3. **Regulations –** The workshop identifies that compliance with the NIS Regulations needs to be met, safety will need to be addressed including OG86 compliance and personal data will require meeting Data Protection obligations of GDPR.
4. **Risk Management expectations** – The potential impact of loss of availability will require 24x7 maintenance response. A high level of cyber hygiene will also be required to match this criticality.

This assessment informed the questions to be asked and the expectations in the Request for Proposal (RFP) and the risks are also reviewed in the context of the RFP responses – which might provide solutions which introduce different/changed risks.

ACT 2b – Request for Proposal (RFP)

Admin Corp produce a RFP ….Request for Proposal. Security engagement for this stage becomes more focused, with Admin Corp homing in on specific areas:

1. **Risk context – As identified by the risk assessment t**he RFP specifies the service and product(s) being requested and this is used by Admin Corp to identify the relevant risks which need to be managed:
   - Risk in security of system design and the design, build and maintenance of devices and software used in the system. Security of network connectivity/logical access by supplier to Admin Corp networks.
   - Security of physical access to systems by supplier staff on site visits.
2. **Bespoke Questionnaire** – Admin Corp uses the risk assessment to develop a custom security questionnaire (cyber security and physical). It uses industry best practices including the IEC 62443 framework, Health and Safety OG86 guidance and also GDPR best practices. They use **common question sets** across suppliers to ensure a level playing field and avoid anti-competitiveness.
3. **Secure design, development and maintenance** – The RFP asks for security information about design, development and ongoing maintenance.
4. **Access Control connection and Encryption** – Because of network connectivity Admin Corp require suppliers to state how they handle **user accounts, remote access, and encryption**.
5. **Security Culture** – including what security training the supplier's staff will have.

Admin Corp's cyber security team analyse the scope of the work defined in the RFP and run the workshop to highlight potential areas of risk specific to the service.

Supply Corp are pleased that Admin Corp are referencing international standards rather than an ad hoc approach. They have good experience of GDPR, however, they have not used the IEC 62443 series before as they work with IT rather than OT systems.

Supply Corp uses products from other suppliers and so will need to have processes to assure the security practices of those suppliers to meet Admin Corp requirements.

Admin Corp will be looking for good identity and access management including strict **role-based access control** and that **VPNs and a security gateway** be mandatory for remote connections. Admin Corp are also after evidence of good security practices beyond technology.

ACT 2c Supplier Assessment

The RFP is issued to 3 suppliers, including Supply Corp, and briefing meetings are held.

From the interactions, and subsequent written responses, it becomes clear that in general the suppliers do not have good experience of specific cybersecurity needs tied to OT systems operating critical infrastructure using standards based on IEC 62443.

In all other aspects Supply Corp meet the RFP requirements and are the preferred vendor.

As a result of discussions between Admin Corp and Supply Corp a principle of a joint approach to security is agreed which will need to be addressed at contract.

Division of security responsibilities between Admin Corp and Supply Corp will be agreed, and a third party specialist OT security company will be engaged to provide review and assurance.

Admin Corp is particularly concerned about system maintenance (software patching) and the availability of 24/7 technical support, especially in the event of a cybersecurity incident.

Admin Corp are faced with a quandary of how to proceed if they cannot find a supplier with the necessary security experience. To check their risk approach, the security team go back to first principles and look at 1) how the third-party service could impact meeting the expectations defined in the UK Cyber Assessment Framework (CAF) and 2) what target Security Levels might be required from the supplier, based on the sensitivity of their data and the importance of the systems. They determine this to be at least Security Level 3 of the IEC 62443 framework.

Before deciding on next steps, Admin Corp use an independent **security assessment maturity service** to evaluate Supply Corp's claims for general security hygiene. This tool helps validate their answers by measuring their cyber security posture against external Internet-facing system benchmarks. The results look good.

Admin Corp decide to approach Supply Corp and see how the security requirements could be addressed through a partnership approach.

Supply Corp are encouraged by the partnership approach proposed by Admin Corp but do have concerns about hidden costs that they may be getting into. They know they need to know a lot more about Admin Corp's systems and current security position.

They also realise that they will need to have deeper relationships with their own suppliers to check they are not carrying hidden risk.

ACT 3 – Contracting and Security Responsibilities

During the contracting process it is recognised that Supply Corp need to be provided with much more information about Admin Corp's systems and security position. This is addressed by the contract having an initial consulting phase where the current position will be documented and a future target agreed.

Key elements of the contract include:

1. **Shared Responsibilities and Patching** – Supply Corp will be responsible for ongoing **patching** and maintenance of the network, but Admin Corp retains control over the monitoring of critical OT systems. To manage this, Admin Corp insists that all patches be tested in a **staging environment** before being applied to the live system.
2. **UK-Specific Regulations** – As Admin Corp is regulated under the NIS Regulation, they require Supply Corp to comply with UK-specific regulations, despite Supply Corp's concerns about this impacting on their European operations. Admin Corp is firm that their infrastructure cannot be compromised to fit Supply Corp's wider business model.
3. **Ongoing Assurance and Audits** –a **through-life assurance** process is to be embedded in the contract, requiring security/compliance status reporting and regular service security audits and **SOC2** compliance from Supply Corp.

Admin Corp's **Finance department** raises concerns about the costs of ongoing maintenance and discussions ensure on fair pricing. They also wanted to spell out exit requirements for end of contract.

Supply Corp looks for back-to-back agreements with systems component suppliers to ensure ongoing maintenance and patch availability. For some major suppliers such as Microsoft, Admin Corp will need to pay for the licences. Some of Admin Corp's expectation will create costs across Supply Corp.

Admin Corp had already included **Legal and Compliance** teams in RFI and RFP to ensure that the contract will be able to reflect their security and safety needs.

Supply Corp was concerned about the expectations for company compliance reporting but are happier with using the American Institute of Certified Public Accountants (AICPA) SOC2 compliance framework as they already have this in place for other customers.

ACT 4 – Consulting, Implementation and Configuration

With the contract signed, Supply Corp begins the consulting phase. There are a list of security procedures and security status of systems which have not been previously documented.

During the consulting process Admin Corp insists on some additional procedures:

1. **Physical and Logical Access Control** – Supply Corp must ensure that all physical and logical access to the network is strictly controlled. This includes onboarding procedures for engineers and clear policies on how access credentials are managed across different systems.
2. **Onboarding and Training** – Admin Corp will introduce a risk briefing similar to their safety briefings. Supply Corp's engineers must be fully trained on Admin Corp's internal procedures and security policies before they can access the systems. This onboarding process becomes essential to avoiding security requirements not being understood.

Integrating the new IP system with Admin Corp's legacy OT systems also proves to be more difficult than anticipated. Supply Corp discovers multiple undocumented legacy assets during an asset audit, complicating the network's configuration. The retained third party specialist OT security company also completes its review of the Admin Corp network and Supply Corp's technical proposals. To enhance security, they propose a new network architecture which is materially different from the current one.

Admin Corp's security team see the opportunity that the contract presents in remediating some known weak security practices in the past.

Admin Corp need to give the proposed new architecture serious consideration, but it is a big step. They decide to put future effort into creating a multi-year strategy.

ACT 5a – Through-Life Assurance risk conversation

Maintenance - Once the new and connected network is implemented and in operation the practicalities of day to day maintenance of the system start to surface. In particular patching not always as straightforward as was envisaged: Changes need to be made when they will not impact operations and need to be done in infrequently scheduled maintenance windows.

Supply Corp has found that some products used in the system are out of support and are trying to obtain security patches.

Assurance - is being performed in accordance with the contract. Since the start of the contract Supply Corp has been providing quarterly status reports on security status and patch levels. These are discussed at quarterly meetings.

At the end of the first year of the contract, Supply Corp write to Admin Corp with their annual assurance letter. This is written in very positive terms, praising the security work of the Supply Corp team and the lack of security incidents. In a closing sentence the letter mentions that some products are out of support, but this does not change the confident conclusion that security processes are going well.

Admin Corp are concerned that frequent requests for patching windows will have the potential of disrupting operations if they were all to go ahead.

Supply Corp find that some system components are now outside of support provided by the vendors.

Supply Corp note that there are a growing number of unpatched vulnerabilities, but record Admin Corp’s decision to accept the risk – a decision which reduces the cost and effort for Supply Corp itself.

Admin Corp are pleased to accept the assurance letter, which they intend to use with their regulators if asked about supply chain security. The comments about some products being out of support is treated with some scepticism as a call for more money. The OT systems are expected to have a long replacement cycle.

ACT 5b –the Incident

Incident - Fourteen months into the contract, an unexpected cybersecurity incident occurs. A vulnerability in a legacy OT system, which had not been properly patched, leads to a breach which could have resulted in an operational incident.

Supply Corp detect unusual system activity which appears to come from some legacy systems maintained by Supply Corp. Admin Corp operate security monitoring but have not alerted on this.

Supply Corp tell Admin Corp what they have seen, and a joint response team is set up to manage the incident. Both must work together to contain the incident, which they successfully manage without service impact.

Lessons Learnt -

Both parties must work out the actions and responsibilities that need to be adopted to address the root causes of the breach. There is also a need for incident management protocols to be developed between Admin Corp and Supply Corp.

The breach underscored the importance of timely patching and regular audits of the system, including legacy OT components. Admin Corp therefore adjusts their approach to require monthly security briefings, formal risk decision points and more frequent patch windows.

When the Supply Corp engineers escalate what they have seen to their line managers, they get a mixed response. Supply Corp's commercial and legal teams are concerned about unnecessarily alarming the customer and liabilities. The contract has a clause which requires Supply Corp to report all security incidents. After some debate of what constitutes an 'incident', Admin Corp are informed.

Both Admin Corp and Supply Corp have some concerns over the cost implications of the resources needed to manage an incident. This was not covered in the contract or services schedule. But everyone agrees that the incident needs managing and now.

Both organisations agree that they need a common and consistent publicity message.

Admin Corp look at their insurance policies to see if the costs of incident response can be recovered.

ACT 6 – Partnership

Building a Resilient Partnership – following on from the lessons learnt review Admin Corp and Supply Corp develop a more collaborative model. A standing security working group is created to jointly review risks and propose solutions. Key initiatives include:

- Creation of a joint strategy for cyber security management including architecting ‘wrap around’ solutions and resilience for products out of support.
- Fostering Continuous Improvement: Regular contract performance reviews and lessons learned reinforced the partnership’s resilience.
- Adapting to Change: Flexible processes allowed both parties to address evolving security requirements without opportunistic charges.
- Maintaining Transparency: Shared reporting mechanisms provided a clear, ongoing view of the threat landscape.
- Aligning with Industry Standards: Collaborative efforts streamlined security requirements and improved efficiency across the sector.

By embedding cybersecurity into every phase of procurement and implementation, Admin Corp successfully mitigated risks, built trust, and created a foundation for long-term operational success. Supply Corp built up their security capability, allowing them to differentiate their services.

References

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
2. https://www.itgovernance.co.uk/iso27001-certification
3. https://www.ncsc.gov.uk/cyberessentials/overview
4. https://iasme.co.uk/cyber-essentials/
5. https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards
6. SCEG Summary of Supply Chain Cyber Security Assurance Standard - https://ritics.org/wp-content/uploads/2023/10/SCEG-Infographic_L1_v1.7_release_Final.pdf
7. SCEG Re-prioritisation of SOC2 Trusted Services Criteria - https://ritics.org/ics-coi-sceg/
8. ANSI/ISA-62443-2-1-2024, Security for industrial automation and control systems, Part 2-1: Security program requirements for IACS asset owners
9. ANSI/ISA-62443-4-1-2018, Security for Industrial Automation and Control Systems – Part 4-1: Secure Product Development Lifecycle Requirement
10. ANSI/ISA-62443-2-4-2018/IEC 62443-2-4:2015+AMD1:2017 CSV, Security for industrial automation and control systems, Part 2-4: Security program requirements for IACS service providers
11. ANSI/ISA-62443-3-3-2013 outlines system security requirements and security levels for industrial automation and control systems (IACS).
12. ANSI/ISA-62443-4-2-2018, Security for industrial automation and control systems, Part 4-2: Technical security requirements for IACS components
13. Security Assessment Maturity Services, e.g.: www.bitsight.com, www.riskrecon.com, www.securityscorecard.com
14. SCEG Guidance for developing Supply Chain Incident Response and Management (Colin Topping) - https://ritics.org/wp-content/uploads/2023/10/SCEG-IR-Man-Supply-Chain-V1.0-final-ac.pdf
15. Example RFI from the energy sector - sceg@csoconfidential.com
16. Energy Sector guidance on creating a risk focused RFP – sceg@csoconfidential.com
17. OG86 - https://www.hse.gov.uk/foi/internalops/og/og-0086.pdf
18. GDPR Guidance - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/security/

Acknowledgements

The Supply Chain Expert Group is a sub-group of the UK NCSC Industrial Control Systems Community of Interest (ICS COI). Information about the community of interest and publications from SCEG and other expert groups can be found at: https://ritics.org/ics-coi/ SCEG publications: https://ritics.org/ics-coi-sceg/

The Supply Chain Expert Group is Co-Led by Paul Dorey & Tania Wallis and may be contacted at sceg@csoconfidential.com

We are grateful for the contributions and review work from SCEG members in producing this document, in particular:

Paul Bailey
Paul Dorey
Clare McBrearty
Chris McGookin
Gordon Robinson
Richard Smith
Mike StJohn-Green
John Thornley
Colin Topping
Tania Wallis

April 2025