



CYBER PATH™
POLICE & ACADEMIA
TALENT HORIZONS



THE
**CYBER
RESILIENCE
CENTRE**
FOR THE SOUTH EAST

Engineering Company

Services Provided: Corporate Internet Discovery

Created For: Engineering Ltd

Report Submitted: 03/05/2023

Student Assessor: Sophie Powell



NATIONAL
**CYBER
RESILIENCE
CENTRE**
GROUP

Contents

Your Assessment.....	1
Executive Summary	0
Risk Summary	1
Corporate Internet Discovery	0
Information about senior stakeholders	1
Physical Premises.....	2
Email Structure and Data Breaches	3
Passwords	5
Website.....	5
Social Media.....	6
Articles and Media Presence	9
There's more to the South East Cyber Resilience Centre... ..	10
About the Cyber Resilience Centre Network	10
Help Bundles and Additional Services	10

Your Assessment

Thank you for entrusting our team at the South East Cyber Resilience Centre to help you. Our unique partnership between Policing, Business and Academia strives to support organisations like yours on their journey to Cyber Resilience. We recognise that this may be the first time you have considered contracting a cyber service and you might be unsure what to expect or how to act on these findings. Our team are dedicated to making the process as simple and transparent as possible, to help you understand the risks highlighted in this report and how to improve on them. Please raise any questions at all with us. We are here to help you learn as much as possible – there are no silly questions here!

Assessment Information	
Service completed.	Corporate Internet Discovery
Assessment Completed By	National Cyber Resilience Centre
Date Completed	03/05/2023
Overseen By	Cyber PATH Supervisors.

Executive Summary

The executive summary identifies the key findings of the report ahead of the technical section and provides an understanding of the content of the report. This section is followed by a Risk Summary which categorises these findings into high-risk, moderate-risk, and low-risk. The technical report can be found after this, which evidence discoveries made during the course of the Corporate Internet Discovery (CID).

The purpose of this CID was to identify the total amount of information available about [REDACTED] Engineering Ltd and its senior stakeholders. The assessment target scope refers to the building and organisation itself, alongside the staff of the organisation. This work has been completed with the support from [REDACTED] Engineering Ltd to [REDACTED]

[REDACTED] This executive summary serves to communicate the primary discoveries that were identified during the assessment, used in collaboration with the risk summary and technical report to provide a clear picture to you.

Discoveries: Passwords, data breaches, and personal information.

A password was discovered in a data breach that used the organisation's name as a part of the password. Passwords serve as the primary defence against unauthorized access to sensitive information. However, shorter, or less complex passwords like the one that was discovered can be easily guessed or cracked by people with bad intent.

Email addresses are used as a backbone of modern business communication and are required for any digitally enabled organisation. Sometimes, email addresses or other identifying pieces of information are released or leaked by people with bad intent – this is one of the causes of what is referred to as a data breach. Breaches that expose details relating to email addresses, usernames, and passwords can contribute to the exposure of sensitive information or incidents. Data breaches can also be used to facilitate more sophisticated phishing attacks from people with bad intent. Email addresses belonging to the company have been involved in eight security breaches that have involved data such as email addresses, passwords, geographic location, job titles, and social media profiles.

A personal address is a piece of identifiable and sensitive information that can be exploited by those with bad intent. The disclosure of this type of information can contribute to more sophisticated social engineering and 'ishing (The umbrella term for all forms of Phishing) attacks. Multiple non-business addresses were included in the incorporation documentation for the organisation, and one of these addresses was verified through the HM Land Registry to not have been sold since this date – confirming the address as the owned residence of one of the officers of the organisation.

Social media is used by businesses to celebrate the accomplishments of organisations as well as reach out to potential clients, and this is done by [REDACTED] Engineering. The Facebook page was identified as "Liking" pages that relate both to the personal interests of the Managing Director of [REDACTED] as well as potentially disclosing parts of their supply chain.

This assessment was a large undertaking that has produced a lengthy technical report. This executive summary cannot summarise the findings in totality. The South Eastern Cyber Resilience Centre team remains available at your convenience to discuss the findings of this report.

Risk Summary

The following table presents a summary of the risks identified throughout the assessment. It can be interpreted based on the colour and order of information. **red** = important and **yellow**=attention required. **Blue**= will likely not pose an ongoing threat but is worth your attention in determining if further action is required.

Summary of High-Risk Findings	
1	A password clearly relating to the organisation has been leaked as a part of a data breach. Passwords are used to authorise users to a given resource or service and are an important part of securing sensitive information. A password was discovered in a breach relating to a company email address, and the password contained the name of the company. This could be used by a person with bad intent to access sensitive resources if the password is still in use.
2	Organisational email addresses have been discovered in eight data breaches. A data breach is a collection of information stemming from unauthorized access, disclosure, or theft of sensitive information – this information varies on the type of breach and can range from usernames and emails to passwords and banking information. Multiple emails at the organisation were discovered to be involved in data breaches that involved email addresses and passwords.
3	Personal Address disclosed via Companies House. Discovered via the incorporation documents of the organisation, the service addresses for the founding officers were confirmed in one instance as the present-day home address of the officer. This verification was done via the HM Land Registry of property sales and allows a person with bad intent to identify the home address of the Officer.

Summary of Moderate-Risk Findings	
4	Comprehensive floor plans available online. As a part of the planning permission process, the floor plans of the organisations building have been made available online. This can be used to navigate the premises and identify the use of the buildings and rooms on the site.
5	Personal use of business social media. Many organisations use Facebook and other social media accounts to share experiences and accomplishments. Using a business Facebook page to like pages related to individual workers or stakeholders reveals personal information, interests, and affiliations. This can be used to craft targeted phishing attacks or enhance social engineering. It was discovered that the business Facebook page likes unofficial pages that disclose personal information about employees.

Summary of Low-Risk Findings	
6	<p>Similarly named business causing cross contamination in data aggregation.</p> <p>When businesses are named similarly or operate in similar fields, data aggregation sites may cross contaminate the information relating to the business. This can lead to misdirected or inaccurate information relating to the organisation.</p> <p>A business was identified that traded using a similar name to the organisation. The legal trading name of the other business was the same as the informal name used to refer to the business on social media, alongside being occasionally in use on the website.</p>
7	<p>Objections to development shared in an article online.</p> <p>An article written by the [REDACTED] Journal titled "[REDACTED]", mentions the organisation twice regarding objections to a planned development.</p> <p>The article shares that several hundred local residents object to the planned development.</p>

Corporate Internet Discovery

Approach

Corporate Internet Discovery is a service used to gather information about a company from publicly available online sources, such as social media, news articles, and government records. This investigation can help businesses to make informed decisions and identify potential risks and threats.

When planning an investigation, the investigator identifies the goals of the investigation, determines the scope of the project with the client, and decides on the tools and resources required for the investigation.

During the collection stage, the investigator uses various tools and techniques to gather information from publicly available sources. These sources may include social media platforms, online forums, news articles, and government databases. The investigator must be thorough and meticulous in collecting information and ensure that all sources are credible and reliable. These can then be impartially reported to you, with an option to debrief and discuss the report after the fact.

Technical Report

The following is an organised discussion of findings that detail the actionable information that has been gathered about the business, alongside identifying the resources and tools used to find that information.

Company Details and Officers

██████████ Engineering Ltd is identified on Companies house as a Machining company with four active officers (One as a double entry), located at ██████████ Engineering Ltd, ██████████ ██████████ ██████████. The registered and advertised phone number of the business as advertised on their website is ██████████. The details disclosed on Company's House about each officer are available below in Table 1.

Table 1 - List of identified employees for ██████████ Engineering Ltd

Name of Director	Job Title	Address	Month/Year of Birth	Mother's Maiden Name	Additional Notes
██████████	Company Director	No	Yes	Yes	Signature identified
██████████	Company Secretary/ Company Director	No	Yes	No	No longer an active Officer.
██████████	Managing Director	Yes	Yes	Yes	Signature Identified

Other Staff

Further details on the employees at the organisation were identified both on Facebook and LinkedIn. Employees identified are shared below. Dates of Birth were almost entirely identified using FreeBMD, an online project that grants free access to a transcribed version of the Civil Registration Index.

Table 2 - Table of other staff at the Organisation.

Name of Employee	Job Title	Address	Month/Year of Birth	Mother's Maiden Name
[REDACTED]	Operations Manager	No	Yes	Yes
[REDACTED]	Chief Quality Inspector	No	Yes	Yes
[REDACTED]	Retired	No	No	No

Shared name of organisation and cross contamination of results

Another organisation exists and trades under a similar enough name that there is some cross contamination regarding the information about stakeholders. Some resources and data aggregation sites wrongly identify the stakeholders of one company as belonging to the other and vice versa. Details of this organisation will not be shared here as they fall outside the scope of this assessment, but it is worth mentioning the trade name is identical to the Facebook page relating to the organisation, which itself differs from the formal trade name of the organisation.

Information about senior stakeholders

The original incorporation of the organisation on Companies House required service addresses, which were filled in at the time with the officers' personal places of residence. Of these, Company Director [REDACTED] address could still be confirmed as his place of residence. This is based on the most recent sale date of the property in 2009, one year before incorporation of [REDACTED] Engineering Ltd. This record is maintained by the HM Land Registry and can be seen (in its redacted form) in Figure 1.



Figure 1 - Information relating to [REDACTED] personal address, which was last sold before incorporation - from which it can be inferred that this remains his personal address. The full address and house prices have been redacted.

The address used by [REDACTED] and [REDACTED] has no held information on the HM Land registry and does not appear to map to an address on Google maps. It is therefore unconfirmed whether this was ever their active place of residence. This can be seen in Figure 2.



Figure 2 - HM Land Registry records do not exist for [REDACTED] listed service address.

Further information that is disclosed about the three officers are their nationality, their date of birth, and nationality.

Physical Premises

Planning permission documents could be identified on the [REDACTED] Council website relating to application [REDACTED]. This publicises eight documents that share the floorplans and design of a building proposed by the Organisation. The full list of files that are available are listed below in Table 3. An example of one of these files is shared below that in Figure 3, and shares the types and models of machines and their location on the floor plan of the ground floor.

Table 3 - Floor plans available by virtue of planning application.

Name of Plan	
[REDACTED]	– Building 1 –
[REDACTED]	– Building 1 –
[REDACTED]	– Building 1 –
[REDACTED]	– Building 1 –
[REDACTED]	– Proposed Site Plan
[REDACTED]	Building 2 –
[REDACTED]	Building 2 –
[REDACTED]	Building 2 –

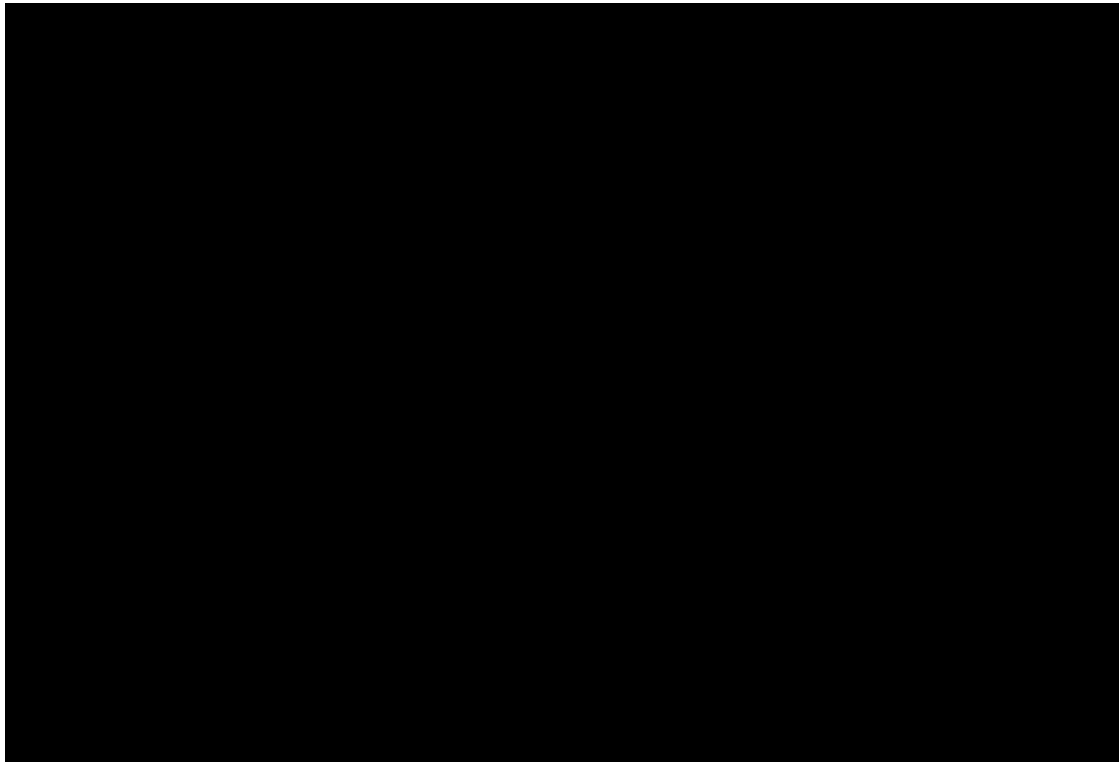


Figure 3 - [REDACTED] - Building 1 - [REDACTED]

Email Structure and Data Breaches

The email structure of the organisation could be identified as *{first}@[REDACTED]* where *{first}* was a single word. The identified email addresses using this domain, alongside the breaches they have been involved in are detailed below in Table 4.







Table 4 - Emails using the [REDACTED] domain, and any associated breaches.


Email Address	Number of Breaches involved in
[REDACTED]	0
info@[REDACTED]	2
[REDACTED]	7

There are seven unique breaches relevant to the organisation that relate to email. Details on these breaches, including the name, data that was possibly involved, and the date of the breach are shared below in Table 5. This also shares which breach applies to which email address. The registered phone number of the company has not been identified as having been involved in a breach, nor the historically listed fax number.

Table 5 - A summary of the breaches that relate to the [REDACTED] registered email addresses.

Name of Breach	Data possibly compromised	Date of Breach	Applies to...
Data Enrichment Exposure	Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, social media profiles	October 2019	[REDACTED]

Kayo.moe Credential Stuffing	Email addresses, Passwords	September 2018	
LinkedIn	Email addresses, Passwords	May 2016	
LinkedIn Scraped Data	Education levels, Email addresses, Genders, Geographic locations, Job titles, Names, Social media profiles	First half of 2021	
Onliner Spambot	Email addresses, Passwords	August 2017	
Verifications.io	Dates of birth, Email addresses, Employers, Genders, Geographic locations, IP addresses, Job titles, Names, Phone numbers, Physical addresses	February 2019	
You have Been Scraped	Email addresses, Employers, Geographic locations, Job titles, Names, Social media profiles	October/November 2018	

It is also worth mentioning that the address  is involved in one 'paste.' Pastes are the first signs of data breaches as they contain partial data from breaches that the leakers can use to prove the authenticity of the breach without disclosing the entire dataset. This does not materially change the amount of information exposed about the email address and is mentioned for the sake of transparency. The extract of the paste involving the email address is visible in Figure 4.

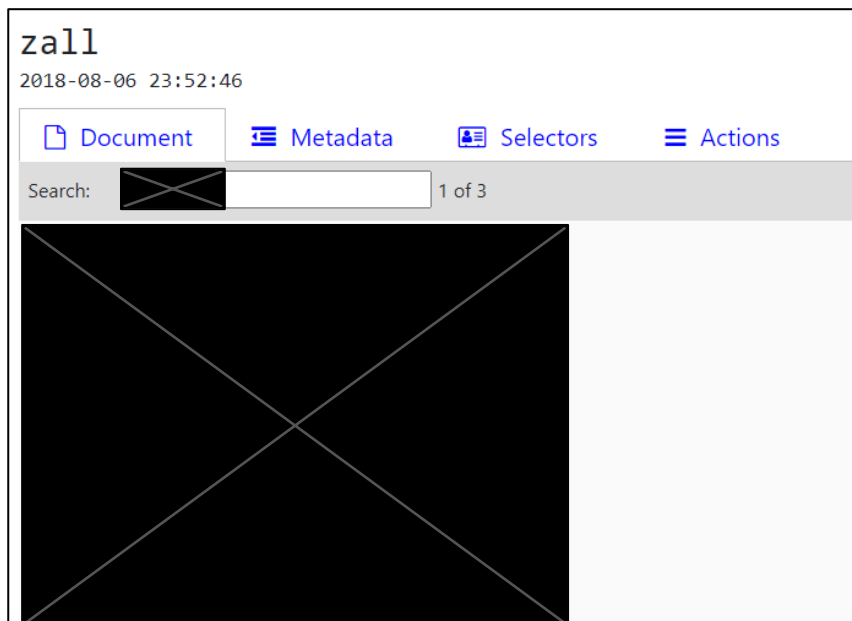


Figure 4 - the 'zall' paste, involving the [REDACTED] email address.

Passwords

One password was discovered that was tied to a breach relating to the [REDACTED] account. This password itself was then discovered in eight breaches according to HaveiBeenPwned.com, and so it is recommended that if this password is still in use, it is changed immediately.

The password in question is [REDACTED]. This password was most likely leaked in either the Onliner Spambot attack in August of 2017, or the LinkedIn attack in May of 2016.

Website

The organisation's website has been archived once by the Wayback machine – which is a digital archiving tool. This archive hosts a version of the website with a footer that shares the [REDACTED] email address that is not in use on the modern site, alongside a Fax number to [REDACTED]. This can be seen in Figure 5.

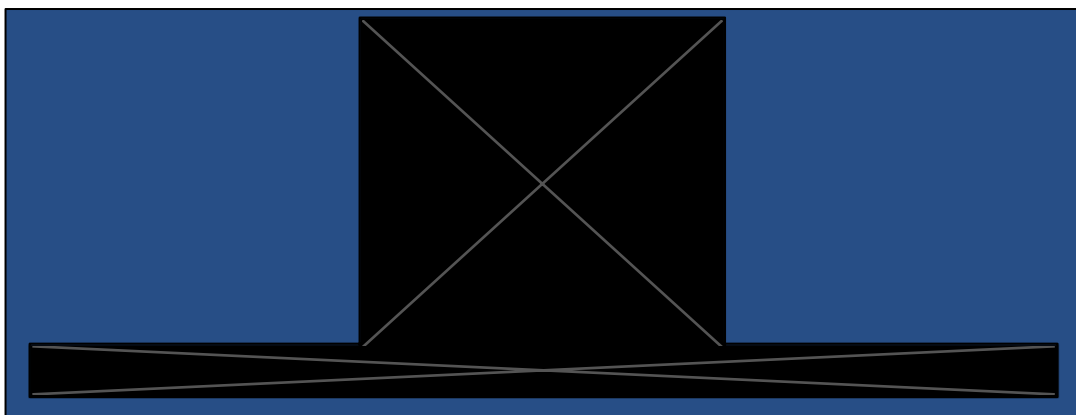


Figure 5 - The footer of the organisation's website as of [REDACTED] 2011.

Social Media

The social media profiles of employees were discovered by searching for employee names and visually confirming that the profiles belonged to the same people.

Facebook has been used to advertise job postings for the organisation from their official page. These job postings included descriptions of work, expected hours and rates of pay for the new vacant positions.

The official page of the organisation could be identified as being run by [REDACTED] and was publicly facing.

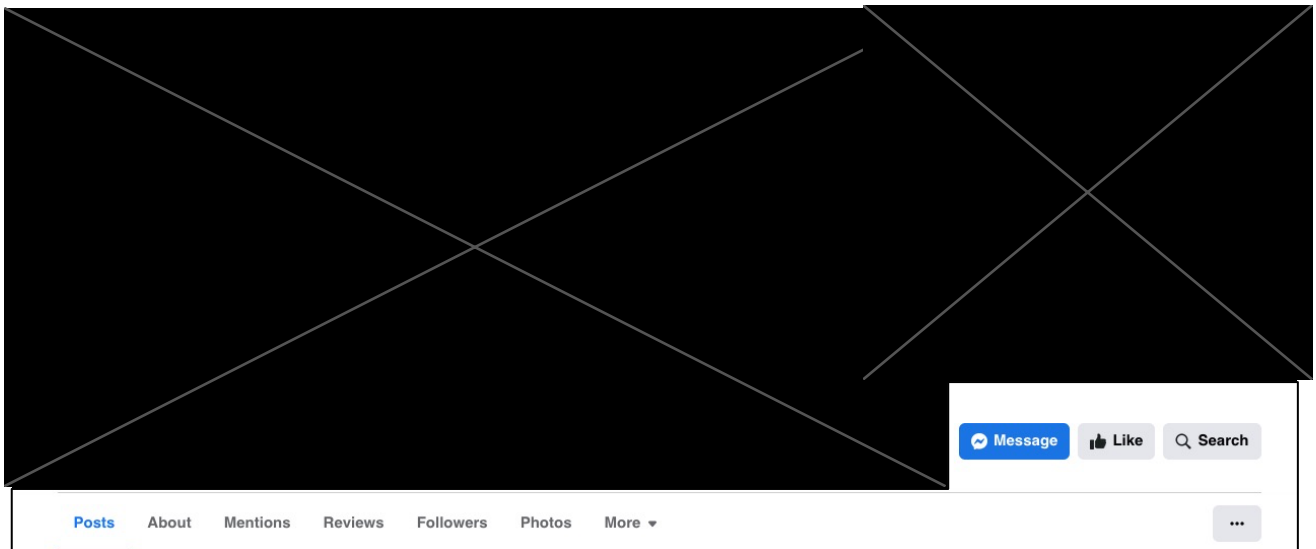


Figure 6 - The organisation's official Facebook page.

The page shared accomplishments and experiences of the team and of the organisation, alongside being used historically to offer job postings for the company, with one example viewable in Figure 7. This discloses the likely pay range of the relevant staff member – in this example, an [REDACTED].

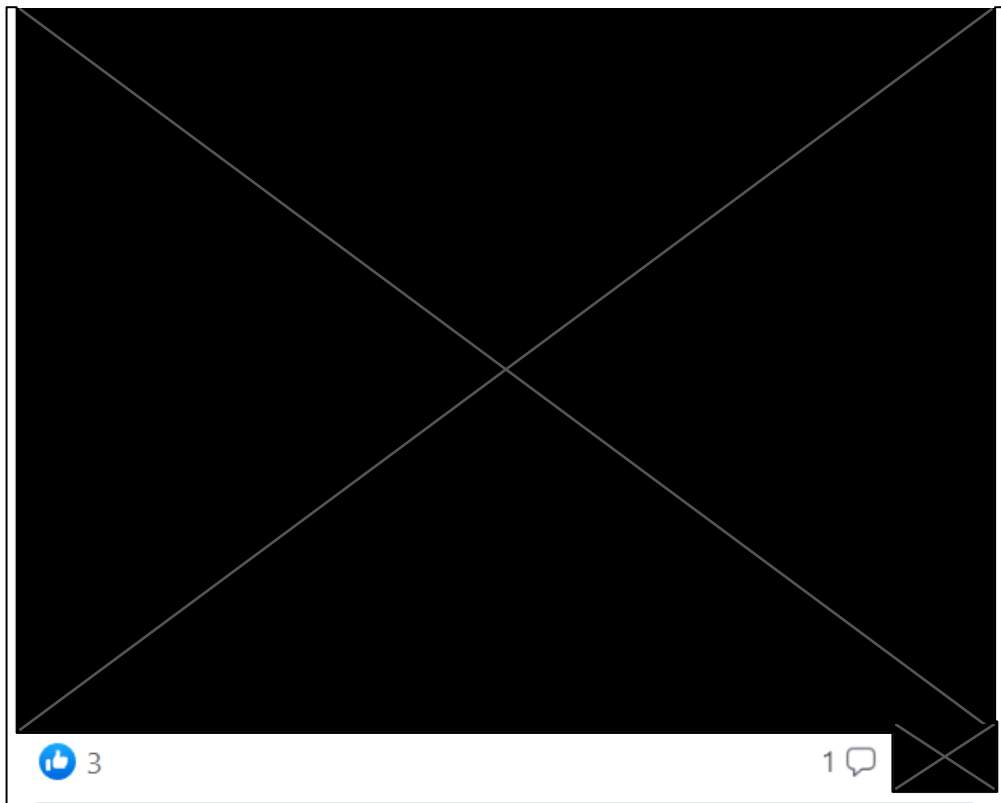


Figure 7 - A job posting from [REDACTED] 2021 for the position of [REDACTED]

Facebook allows pages to “Like” other interests or pages, and the organisation’s Facebook page was discovered to have liked three schools. The identified schools were [REDACTED], [REDACTED], [REDACTED] and [REDACTED]. Some of these pages are unofficial and can be seen in Figure 8.

[REDACTED] has listed the [REDACTED] as the school he attended on LinkedIn. It is not best practice to identify schools that may be relevant to the stakeholders in the organisation, and this should be considered if the other two schools liked by the page relate to family members.

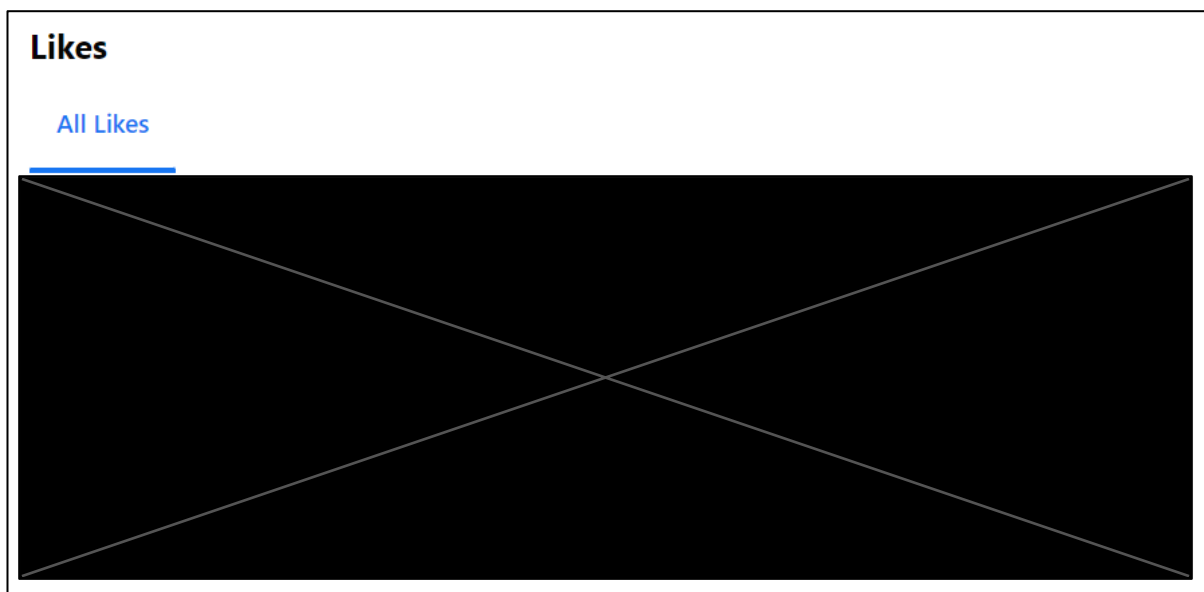


Figure 8 - The pages that the organisation's Facebook page "Likes".

The organisations Facebook page follows a locksmith company called [REDACTED] (Viewable in Figure 9) and the director of that organisation alongside the director's partner frequently like posts made by the Organisation. This locksmith frequently posts photos of the keys it has cut for its customers.

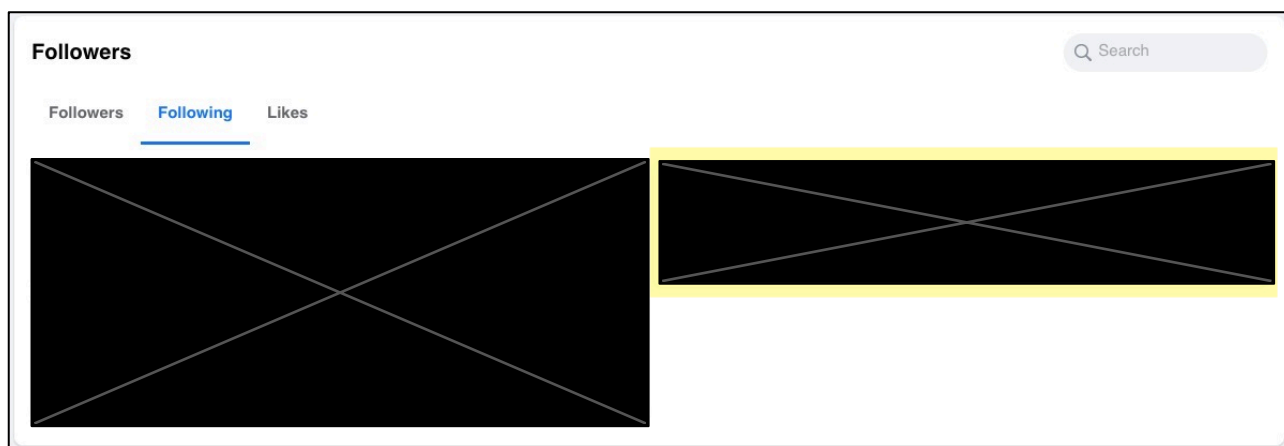


Figure 9 - [REDACTED] Ltd, followed by the organisation Facebook page.

The social media account was also used to share another existing relationship with their supply chain, increasing the threat surface of spear-phishing attacks from a person with bad intent. This is shown in Figure

10, where a machinery organisation shared the model of a piece of machinery alongside the name of the organisation, a visiting senior stakeholder, and the names of the staff involved in this relationship.

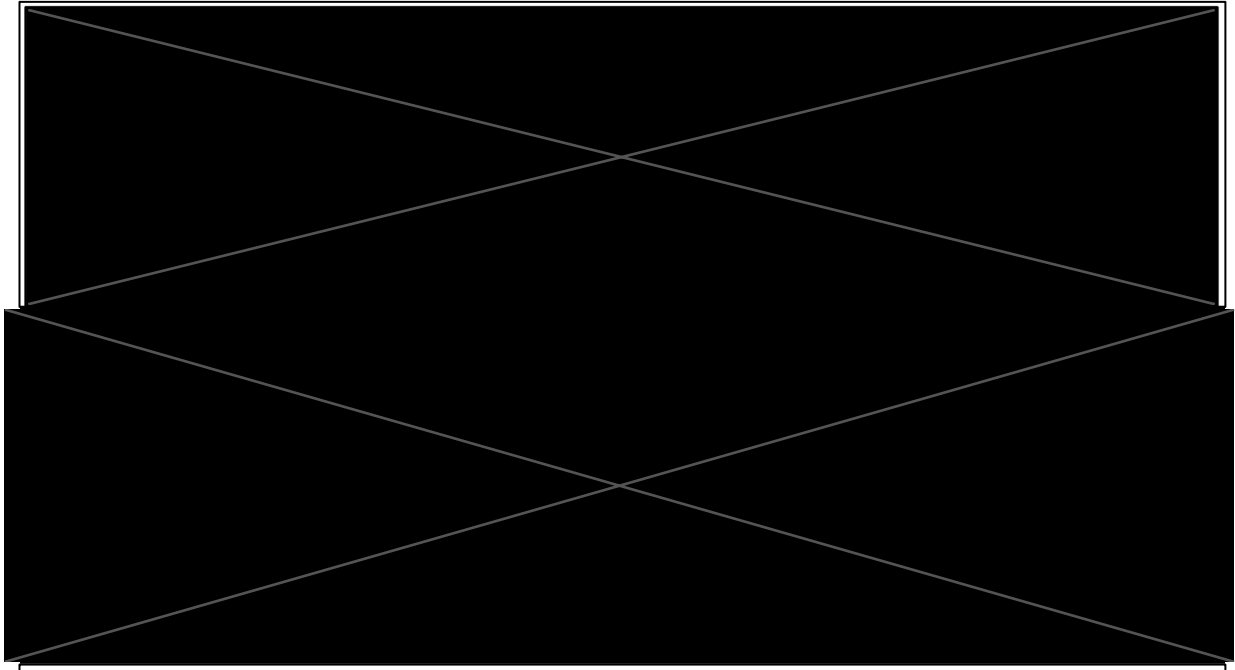


Figure 10 - A post from [REDACTED] Ltd, advertising that it sold a [REDACTED] to the organisation.

Articles and Media Presence

An article written by the [REDACTED] Journal titled “[REDACTED]”, mentions [REDACTED] engineering twice regarding objects against the [REDACTED]. The article shares that several hundred local residents object to the planned development that involved and relates to the organisation.

The article mentions [REDACTED] who say that the community “[REDACTED]” at the prospect of a [REDACTED]. He also mentioned that he has not seen anyone in favour of the development.

There is more to the South East Cyber Resilience Centre...

There are many additional ways to engage with SECRC. If you have not already, you can register as a Core Member of the South East community, which is free of charge. This membership includes practical, government-approved guidance, as well as regular information updates to keep you informed of our other help and services on offer, including:

- **Educational Events** - we run regular webinars and events on a range of topics relevant to your small business or third sector organisation.
- **Affordable solutions** - we offer a range of paid services like this one which are designed to address the most pertinent risks affecting SMEs, as identified by policing and Government.
- **Cyber Essentials Certification** - we have a Trusted Partners forum, which is made up of IASME approved Cyber Essentials Certifiers. If you are planning on achieving Cyber Essentials or Cyber Essentials Plus certification, we can refer you to the Trusted Partners forum of local suppliers in the region that provide this.

About the Cyber Resilience Centre Network

The National Cyber Resilience Centre Group and Cyber Resilience Centres are funded and supported by the Home Office and policing in a not-for-profit partnership with the private sector and academia to strengthen our national cyber resilience across SMEs and the supply chain.

At a national level, NCRCG is building a coalition of police, government, large employers and organisations, and academia to ensure a collaborative and coherent approach to cyber resilience.

NCRCG and its National Ambassadors and the CRC network are committed to investing in the next generation of cyber experts. As such, NCRCG has launched Cyber PATH in partnership with the CRC network and over forty-five universities.

The nine CRCs operate across England and Wales. They serve SMEs in their locality helping to build cyber resilience against threats that are specific to them. Cyber PATH empowers students to work with their regional CRC in meeting the requests brought to them by local businesses.

Each CRC retains the freedoms to deliver tailored, trusted, and affordable support, with NCRCG providing insight and solutions at a macro level.

You can learn more about the work of the NCRCG [here](#). We can help your own customers and suppliers too, so spread the word.

Help Bundles and Additional Services

If you are ready for more support, we offer free Core membership and a selection of Help Bundles which include paid services and 12 months of support. This includes:

- Full website vulnerability testing
- Policy Review
- Staff awareness training

Visit our selection of Help Bundles and Services [here](#). You can also engage with us through our social media channels – find us on [LinkedIn](#), [Facebook](#) and [Twitter](#).

Contact us at enquiries@seccr.co.uk if there is anything else we can help you with.