

**Resilience First** 

Briefing & Workshop – 12 March 2019 – Summary

Measuring cyber resilience across subsidiaries and suppliers

## Introduction

This briefing and exercise, kindly hosted by Facebook in London, was designed to help attendees think about resilience across their chain of suppliers and partners, and provide practical advice for managing any risks. Around 50 people attended.

The main area of focus was on resilience to cyber threats such as handling sensitive information, viruses and hacking.

## Discussion

The first presentation was from Peter, Deputy Director Lead on Supply Chain at the National Cyber Security Centre.

He outlined the NCSC's aim of removing avenues for cyber attack from the supply chain, highlighting that two major attacks the NCSC had dealt with have been introduced via Managed Service Providers and Communications suppliers to their extensive customer bases.



According to a survey conducted in late 2018 by the Ponemon Institute, 56% of

organisations had a breach caused by a supplier. Only 18% of organisations realised their suppliers were sharing sensitive information.

Key steps that organisations can take include:

- Identifying who their suppliers are.
- Rating them for risk: who are the really critical ones? This recognises that it is impossible to understand fully every supplier, especially if you have hundreds.
- Insert Cyber Security clauses in contracts.
- Asking for Cyber Essentials.
- Educating users.

Under GDPR there is a duty to notify the Information Commissioner of any breach within 72 hours. Peter also advised notifying the NCSC as well: while not a regulator, it may be able to assist or the information provided may be valuable to the wider business community.

Resources to help with understanding and managing risk and improving resilience are available on the <u>NCSC website</u>, including a guide to the Cyber Essentials scheme, and a useful infographic is attached to this report.

## Exercise

Kevin Duffey of Cyber Rescue conducted an exercise with the attendees to help them think about cyber risks and vulnerabilities.

Using the Slido polling system, attendees were asked who they trust with sensitive information. The results were:

Who do you trust with sensitive data? (Select all that apply)	029	
Your boss 69 %		
Your team	<b>9</b> 3 %	
Your IT Department 31 %		
Your Supplier(s)		

The example of an organisation's HR department was used to demonstrate the sheer breadth of contacts:

- Recruitment, vetting and payroll agencies;
- Pension providers;
- Private health care providers;
- Other benefits providers;
- Training providers;
- Coaches and mentors;
- Staff survey providers;
- Unions;
- Legal experts.

Insight from Cyber Rescue research showed some of the issues associated with sharing information.

Who do you trust with sensitive data?			
1)	Your boss	63% of CEOs admit to clicking links by mistake	
2)	Your team	22% of staff clicked a phishing link in the last year	
3)	Your IT Department	17% of those that spend < 10% of IT budget on security identified a data breach in last 12 months	
4)	Your Supplier(s)	416% annual growth in number of records breached via a supplier or other third party	

Kevin also highlighted that for organisations that spend more than 10% of their IT budget on security, the likelihood of detecting a break doubled.

The second discussion point looked at what attendees thought were the most effective ways to engage suppliers and review their resilience to cyber threats. Options included:

## How best to review suppliers?

Attestation:	60 questions completed each year by 1 person at supplier	
Awareness:	1 hour online compliance training & assessment by all staff	
Certification:	8 hour audit completed every three years by external reviewer	
Discussion:	1 hour meeting where supplier explains security governance	
Cyber Range:	8 hour competition for IT staff, with scores & feedback	
Pen Testing:	10 days of probing each year, of 10% of the applications in use	
ScoreCard:	365 days monitoring, scores & feedback on all external systems	
Simulation:	2 hour simulation of executive decisions during a breach	

Participants were encouraged to think about their 'attack surface': the size of their IT network, added to that of their suppliers and other partners.

He also demonstrated a scorecard system that can be used to drill down into an organisation to understand where its risk areas lie.

Participants noted that while due diligence on a company is important, just as important is reputation and the need to

Security Summary Report Prepared on anizote Degreed on anizote Endowned parentee	• OVERED & Y S Sectorpresent Bis on party the non-monitoring and and another independent for the price of an another another independent for the price of an another independent for the price of an another another independent for the price of an another independent for the price of an another another independent for the price of an another independent for the price of an another independent for the price of an
1075	Industry Comparison
Threat Indicators	
Description	1

have a relationship with suppliers and partners to build trust and encourage openness and honesty.

Kevin's slides can be viewed <u>here</u>.

The event was closed by former UK police lead for economic crime and cyber protection, Chris Greany. He reminded the audience that at its heart, any cyber risk is still a human problem, saying: "Cyber is on the inside, not the outside. Everyone worries about letting cyber risks in. But the problem is almost certainly in your organisation already."

You can also see a timeline of the event on the Resilience First Twitter feed @ResilienceFirst.