10 MAY 2021 | EDITION 3

DEFUSE NEWS

A weekly update of relevant issues

Facebook's encryption will cost lives in fight against terror and crime*

Neil Basu, a friend and former boss of mine featured in Saturday's Times discussing the subject of Facebook's plans to install end-to-end encryption and the potential impact of this on investigations. Facebook's own head of global policy management has admitted to a Parliamentary committee that end-to-end encryption on all its messaging products will lead to continued exploitation of some of the British children it would otherwise help to safeguard. Encryption involves mathematically encoding data, in this case Facebook or Instagram messages, so that only someone with a secret key can read it. The technique relies on mathematical puzzles that require a gargantuan amount of processing power to break without the key.

Facebook argue that they want to introduce this end-to-end encryption to keep people safe from hackers and criminals. Law enforcements argue that they are concerned that this same process will make it more difficult, if not impossible to conduct lawful investigations....and keep the public safe.

Neil Basu, Britain's most senior counterterrorism officer, states in the Times article that he believes that an all-society approach is needed to prevent terrorism and serious crime. He is a man of utmost integrity as well a brilliant detective, and as such I will take his guidance on this matter as words of wisdom. There must be a way that tech companies can enhance security whilst ensuring that that security doesn't compromise lawful investigations to be conducted, collectively increasing our safety.

D E F U S E

FEEL SAFER IN PUBLIC LIFE

+44 (0) 2072930932

enqs@defuseglobal.com

www.defuseglobal.com

How do you *'Defuse'* a Threat or reduce Risk?

How many really understand the differences between security terms such as **Risk, Threat and Vulnerability**? These are important terms that any security professional must know and understand how they fit together.

The term **Risk** is made up by a combination of the **Impact** and **Likelihood** of an 'attack'. The word attack conjures up an image of a physical assault of some description, but can equally be applied to a reputational, financial, psychological attack too.

The **Impact** and **Likelihood** are derived from the **Threat** and **Vulnerability** and these are derived from the **Intent** and **Capability** of the threat actor.

There are two component parts to a **Threat**....**Intent** and **Capability**, both of which must be present for a **Threat** to be considered viable. Remove or *'defuse*' either one and the Threat is reduced or disappears.

The **Intent** is their desire, the reason why they want to cause harm. It may be the result of ideology, greed, anger or any number of emotions or reasons. Targeted violence is often, but not exclusively driven by a grievance of some description, which forms the **Intent** or motivation. This **Intent** forms the basis of the Prevent element of Contest which is the United Kingdom's counter-terrorism strategy, but is equally applicable to a domestic dispute or an argument is the street.

What is it that has motivated or inspired or caused this dispute or grievance? Resolve that and the **Intent** dissipates and with it any **Threat**.

Intent is just a thought process, it is however, the foundation of any **Threat**. For the **Threat** to be serious, and perhaps to justify ' level' of T**hreat** there must be C**apability** to action their **Intent.** Eliminate the **Capability** and the **Threat** dissipates.

If we are unable to reduce the **Threat** because we cannot *'defuse'* their **Intent** or their **Capabilities**, we are then left with the option of assessing the **Vulnerabilities** of the subject of the **Threat**, to reduce any likelihood of a successful attack.

The **Vulnerability** is the weakness of gaps in the potential victim's defences, their Achilles Heel, or chinks in their armour. Everyone and every organisation has **Vulnerabilities** and it is the job of the **Threat** actor to seek out and exploit these, and the security professional or agency to counter that. The level of that response is proportionate to the **Threat**.

The **Threat**, **Vulnerability** and **Impact** all go towards assessing the **Risk**. **Risk** can be defined as the amount of harm that is likely if no action is taken. **Risk** is an uncertain future event, that may or may not happen.

Think if it like a 3 legged stool. Remove one leg and 'it' falls over.

(full article available here: https://www.defuseglobal.com/how-do-you-defuse-a-threat-or-reduce-vulnerabilities-and-or-risk/)