nagalro
children seen and heard
Article in *Seen and Heard*, Volume 33 | Issue 2 | 2023

WHAT EVERY ISW MUST KNOW ABOUT RANSOMWARE AND CYBER-SECURITY

Rodney Noon

Introduction

Imagine this. You have three court reports to file tomorrow morning. You switch on your computer and up comes a screen that reads:

Ooops, your files have been encrypted!

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

If you want to decrypt all of your files, you need to pay.

You have only three days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

Nothing on your computer works and no files can be opened. This is happening to people, businesses and organisations across the world. It could happen to you.

Last year, Nagalro's insurers made it clear that their professional indemnity and public liability block policy would no longer cover cyber risks, such as hacking or ransomware. This means that ISWs need to understand what to do to keep safe in this environment, because their bank balances and reputations are exposed. It need not be difficult to do and requires more common sense than technical know-how. However, when you are busy it would be very easy to say, 'I'm just a little one-man-band. No one is going to bother with me. I don't need to worry about all this.' Hopefully, I can explain why that is not only factually wrong, it is the exact mindset that a huge number of international criminal organisations depend upon for their success.

Unless you have no access to email and have no connection to the internet, your computers are potential targets for criminals around the world for theft and extortion. It is a fallacy to think that you or your organisation is too small, because, in most instances, the victims have not been specifically selected as targets. Many millions of emails can be sent out, quite randomly, containing an infected attachment or a link to be clicked on. The criminals will attack *anyone* whose computer they can get access to. If only a fraction of a fraction of one per cent of the emails are opened,

the operation will have been a success. Often, we are not selected for attack, we self-select by leaving our 'doors and windows open' and that realisation gives us the best basis for defence.

What is ransomware?

This is the current type of cyber threat that is presently causing significant concern amongst bodies such as the UK's National Cyber Security Centre (NCSC) (part of GCHQ) and the United States' Cybersecurity and Infrastructure Security Agency (CISA). The NCSC defines ransomware as 'malicious software that prevents you from accessing your computer (or data that is stored on your computer)'. Payment is usually demanded from an anonymous website and usually in a cryptocurrency such as bitcoin.

There are many different ransomware programmes, or 'strains'. They are so numerous that their developers can sell them to anyone who wants to set up in the extortion business. Recently, the National Crime Agency (NCA) investigated just two strains of ransomware used in the UK. There were 149 *known* victims and at least £27m was extorted. In February 2023, CISA warned that North Korea, otherwise known as the Democratic People's Republic of Korea (DPRK) is using ransomware as part of its national economy.

> *'The authoring agencies assess that an unspecified amount of revenue from these cryptocurrency operations supports DPRK national-level priorities and objectives, including cyber operations targeting the United States and South Korea governments—specific targets include Department of Defense Information Networks and Defense Industrial Base member networks.'*

On 10 February 2023, the NCSC reported that seven Russian cybercriminals have had sanctions imposed against them for the development or deployment of ransomware strains used to target the UK. The NCSC warns that:

> *'Ransomware is the most acute cyber threat the UK faces and attacks can have devastating consequences on an organisation's operations, finances and their reputation.*
>
> *'Organisations should take immediate steps to help mitigate ransomware attacks by following the NCSC's guidance.'*

On 24 February 2023, a further threat report from the NCSC details several ransomware groups, based in China, which are launching attacks in Europe. The NCSC draws attention to a joint report from the European Union Agency for Cybersecurity (ENISA) and the Computer Emergency Response Team (CERT-EU):

'
