Why now? Sunday Times Sept 2016

by cyber blackmailers

John Boothman

CYBERCRIMINALS from Eastern Europe are holding Scottish companies to ransom by hacking into their computer systems and disabling their access to files unless they make a payment.

Police Scotland has warned of a rise in ransomware, malicious software that is hitting firms around the world. Scotland is said have become a significant target due to its high proportion of small- and medium-sized enterprises (SMEs), with some companies opting to pay to avoid the damage their fear it could cause their business.

One insurance broker in the Glasgow area, who wished to remain anonymous, told The Sunday Times of his experience, which cost his small firm thousands of pounds and took more than a month to fix.

"Out of the blue I was alerted by staff to a problem with our computers. I called in IT and we quickly established that we were unable to get into the shared drive, which contained thousands of our client files," he said. "IT said there was a demand from Russia for £750 and a threat that if we didn't pay within four days the ransom would double. The note said I should open an account and pay by bitcoin.

"I spoke to a number of business colleagues at the golf club and they suggested I pay and hope it goes away. I considered it but decided to go to the police. Two young policemen turned up, they said they get this a lot, and advised me not to stump up."

He called in a cyber security expert who worked remotely on the problem around the clock for 48 hours.

"The specialist unlocked half of the files, most of the rest were accessed from backups, but it took four weeks to get fully up and running," he said.

"I thought we had significant security and were really well protected. But it appears the attackers update their software all the time and can overcome these precautions.

"I've updated our security software and installed new backups, but all in it has cost a few thousand pounds, never mind the stress and hassle."

He is aware others are suffering similar attacks, citing a Glasgow company that paid £20,000 to recover its files.

Police Scotland said it acknowledges the problem but added the number of cases remains small. It wants enterprises to give a greater priority to cybersecurity.

Detective Superintendent Willie Cravens of Police Scotland's specialist crime division said: "Although such instances are rare, businesses need to place a greater emphasis on prevention, testing and training to put in place several layers of cyber security."

Richard Brooks

IT IS thought to be the valuable collection of 20th-century art asse in Britain. The Royal Academy's forthcomi exhibition of painting abstract expressionist feature works estimat worth more than £1br

The 165 works, to g display on September include 18 by Jackson Pollock, 17 by Willem Kooning and 13 by Ma Rothko — each of wh works have sold for u nine figure sums.

"Within 20th-cent it is probably the mos valuable exhibition ev said Edith Devaney, a curator of the show. ' are some of the jewel crown of abstract expressionism."

The exhibition fea painting by Pollock t to contain the artist' blood and several ca so large they will be through the front e

Why now? A steep learning curve?

‘ I NEED CYBER!’

© Many in our industry

Why now? TALK TALK £400,000 fine

Information Commissioner Elizabeth Denham commented -

"Today's record fine acts as a warning to others that cyber security is not an IT issue, it is a boardroom issue. Companies must be diligent and vigilant. They must do this not only because they have a duty under law, but because they have a duty to their customers," she added.

Why now?

But it's not only the household names at risk - 74% of UK businesses in 2015

University of Greenwich **MNH Platinum**

Guernsey **Lincolnshire County Council**

General Data Protection Regulation

- New regulations in **May 2018**
- Increases responsibility for data
- Increases costs of a breach significantly

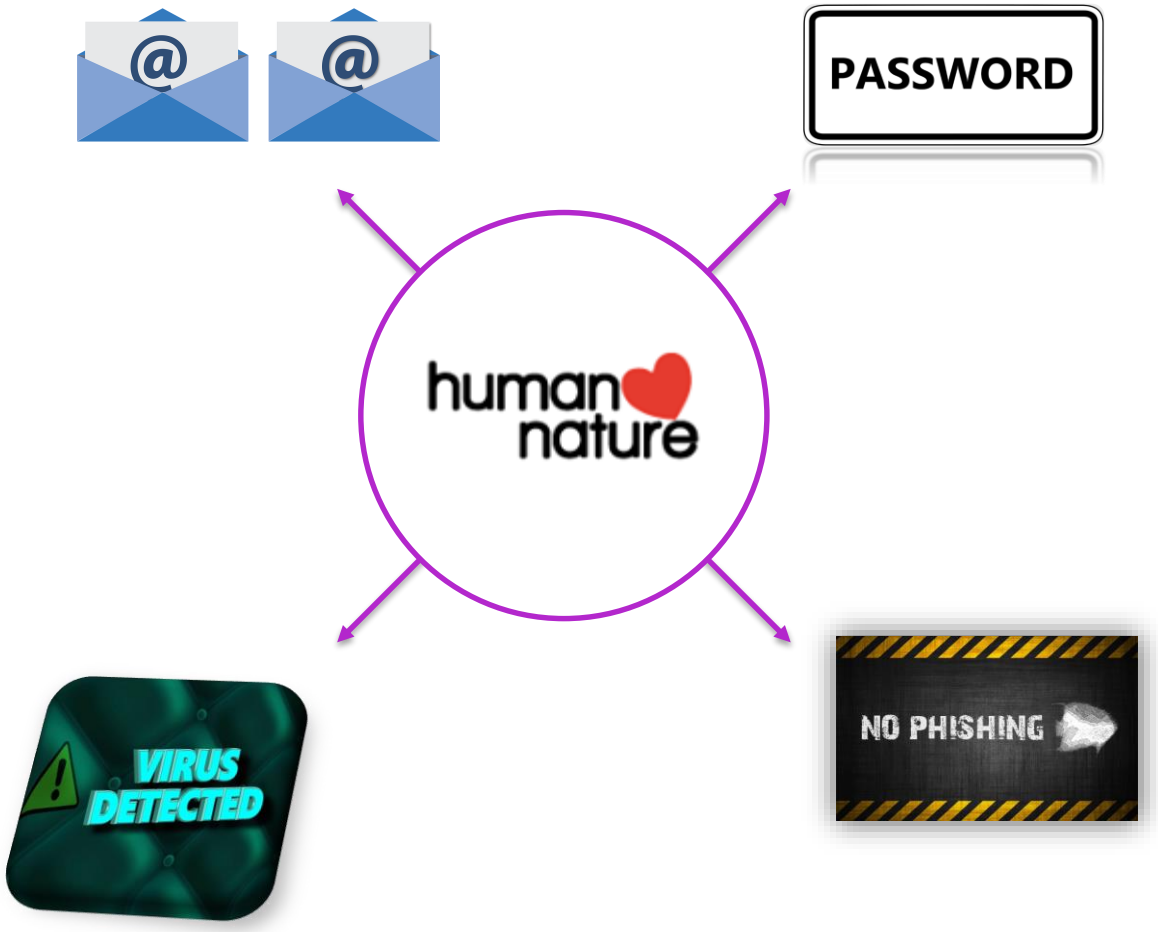
Utilise our CII resources!

Everything you ever wanted to know about the impending General Data Protection Regulations but were too embarrassed to ask...

This essential 30 min Faculty video focuses on the General Data Protection Regulations which will come into force on 25 May 2018.

Watch the full video here >>

Everyone has a Cyber exposure



AROUND

52%

OF

BUSINESSES **THINK** THEY HAVE CYBER COVER

IN REALITY **LESS THAN**

10%

ACTUALLY DO

Our clients have evolved

The coconut represents old style IT security;
Like a fortress this fruit is hard outside but soft inside

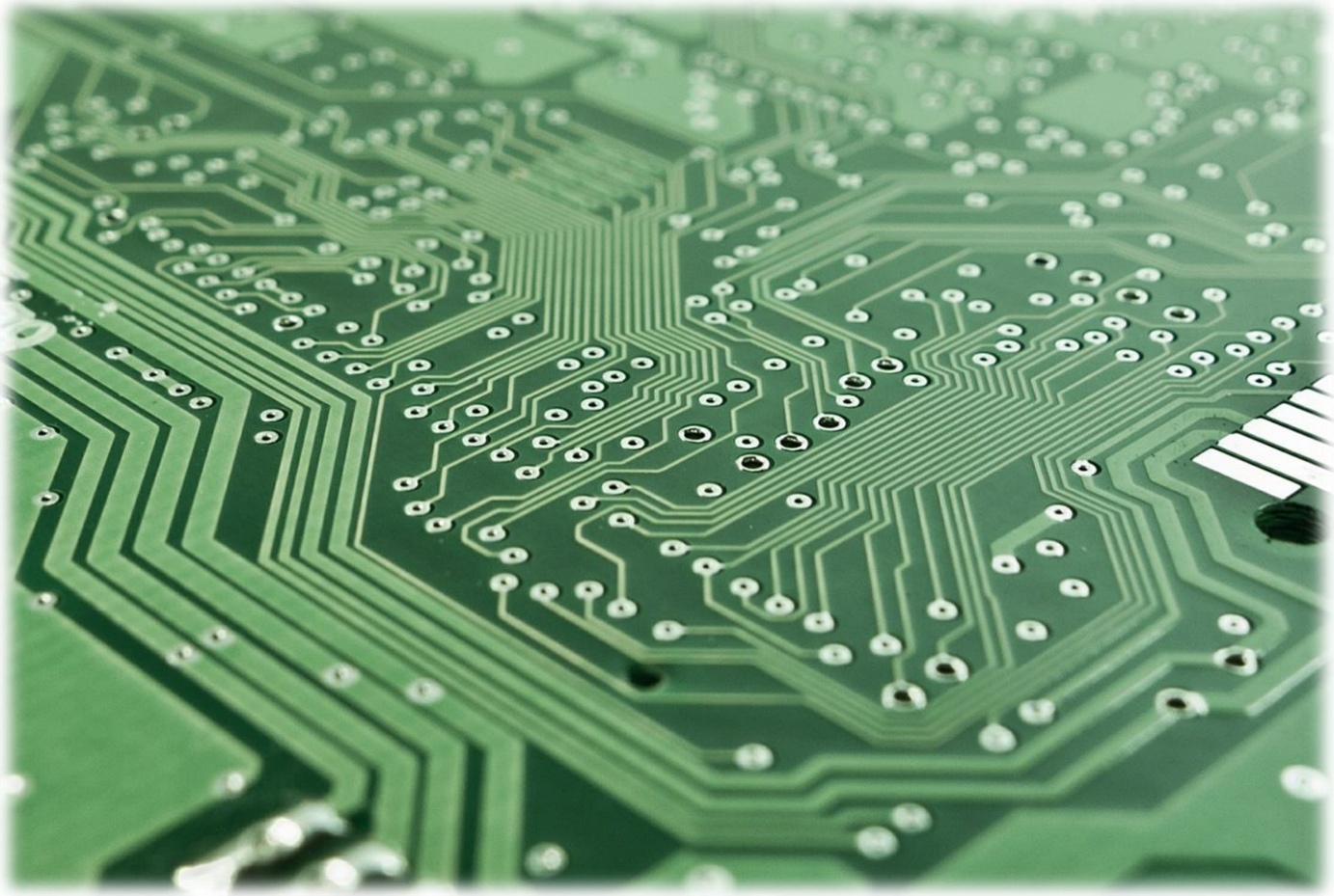
The mango represents the new cyber age approach to IT security.

Organisations that work towards the mango model and harden the core of their IT:

- ✓ Understand their important data, like products, clients and contracts
- ✓ Can identify their key processes like Research & development, sales tools etc.
- ✓ Protect their critical applications; finance, HR
- ✓ Can identify other vital infrastructures and systems
- ✓ They have a business continuity or disaster recover plan that includes a Cyber Event.
- ✓ They know which Cyber event will impact them the most.

CYBER ISSUES – THE IMPACT TO YOUR CLIENTS AND THEIR CLIENTS ARE IMMEASURABLE

THE CLIENT HAS LOST SOME DATA



RANSOMWARE – this is happening

OUR BOOKING SYSTEM HAS BEEN CORRUPTED

IN OUR MARKET

- Cyber Liability is market news, but there is no market standard
- While there is widespread acceptance that a vulnerability exists, there is often little understanding of what that vulnerability is

TWO WAYS TO LOOK AT CYBER

Cyber Risk can be split into two main sections:

- Network Security Events
- Privacy Related Events

Data Liability Event

Loss or suspected loss of third party data for which the client is legally responsible

Breach of worldwide privacy legislation

E.g.
Lost laptop
Stolen storage device
Rogue employee

Network Security Event

Negligent or inadvertent transmission of malware to a third party

Negligent failure to secure the network or computer system which results in unauthorised access

E.g.
Virus transmission
Hacker attack
Extortion

UNDERPINNED BY BUSINESS INTERRUPTION COVER

Cyber First Party Covers

What issues should you and your clients consider:

Forensics – what has happened – investigate

Legal Counselling and PR costs – do you need help – what are next steps

Voluntary notification costs

Data Restoration costs

Business Interruption

Cyber Third Party Covers

What issues should you and your clients consider:

Regulatory fines and penalties

Damages – claims from data subjects

Notification – mandatory notification costs

Legal Costs

EU GDPR May 2018 - this will ‘drive’ client interest

WHAT DOES A CLAIM LOOK LIKE?

Cyber Extortion

IT Forensics

Rescue

24/7 Helpline

PR Advice

Legal Advice & Defence Costs

Cyber Business Interruption

Data Restoration Costs

Restoration

Notification Costs

Credit & ID Monitoring Costs

Response

WHAT IS THE COST OF A CLAIM?

Do they even know what to do, who to call? Delay increases costs.

THE COST OF FIXING A DATA BREACH OF 1,000 RECORDS IS BETWEEN

£33–£35

PER RECORD*

And that's just the cost of looking after data breach victims

*Verizon Data Breach Investigations Report May 2015

CYBER THEFT

COVERING YOUR CLIENTS OWN FINANCIAL LOSS

Then versus now……

Cyber Risks and Cyber Theft

Cyber Risks covers your client's intangible risks associated with a Data Liability or Network Security issue – and any resultant exposure and costs

Cyber Theft already being covered under Commercial Crime products

Needs and demands critical what is your client concerned about? Sell the appropriate product

A Combined Cyber and Cyber Theft Policy is not a panacea to all ills. What about employee fraud, or fraud losses that do not have a Cyber mechanism as their proximate cause

The devil is in the detail – so let's explore……..

CYBER THREAT

EMAIL CLOAKING? - CYBER OR COMMERCIAL CRIME?

“IT IS EASIER TO TAKE ORDERS OVER THE NET”

FISHING or PHISHING? And now SMISHING!!!

COMMERCIAL CRIME COVER IS VITAL

Commercial Crime has a broad Insuring Clause

- RSA Commercial Crime – Insuring Clause reads – criminal, fraudulent or dishonest taking 'by any person'
- Cyber frauds are unlikely to be covered under Fidelity wordings or under 'Crime' extensions to Management Protection contracts
- Cyber wordings are evolving – on Theft cover – be careful to read the terms and conditions
- Be cautious on 'knowingly surrendered' exclusions – these will really impact the cover where an Insured has been duped
- Be cautious on 'social engineering' exclusions or sub limits

The Devil is in the detail

WHAT BARRIERS DO WE HAVE IN SELLING CYBER AND COMMERCIAL CRIME?

BE RESILIENT – CLIENTS MAY TAKE THIS APPROACH

WHATS NEXT?

WHAT NEXT?

- **This is PROFESSIONAL ADVISE**
- **Our clients businesses have EVOLVED – have we?**
- **Don't wait for your client to ask, or someone else will**
- **Resiliency is the key – both for the insurance industry and our clients**
- **EU GDPR will be the 'EUREKA' moment for Cyber – 25th May 2018**

QUESTIONS