

UPCOMING EVENTS



The Insurance
Institute of Leicester
Chartered Insurance Institute

(GI) Lunchtime Seminar - The Life of a Major Risk

🕒 **Wed 07 Nov 12:15 pm – 1:45 pm**
👤 Kevin Dinsdale, Crawfords

📍 Mercure Leicester The The Grand Hotel

With Kevin Dinsdale - Crawfords

[View event details](#)



Lunchtime Seminar 03/10/2018

An overview on how businesses are exposed to cyber risk.

Matt Sumpter – European Underwriting Director CNA Hardy

[ALL] 104th Annual Dinner

🕒 **Fri 09 Nov 6:00 pm – 1:00 am**
👤 To be confirmed

📍 Marriott Hotel

President Chris MacLeod cordially invites you to the Insurance Institute of Leicester's 104th annual dinner.

[View event details](#)

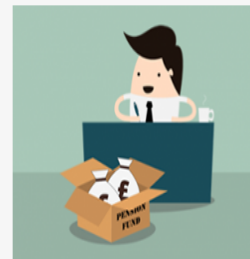


(PFS) Breakfast Seminar - 5 Best Practice Steps for a Defined Benefit Transfer

🕒 **Wed 14 Nov 7:45 am – 9:00 am**
👤 John Corbyn, Old Mutual Wealth

📍 Hilton Hotel

With John Corbyn - Pensions Expert - Old Mutual.



Special thanks to today's sponsors:

BHIB
INSURANCE BROKERS

Cyber



Matt Sumpter – European Underwriting Director – Technology & Cyber Risks

Cyber – What is it ?!



Coverage triggers differ from traditional Fire and Theft

Unauthorised Access

Computer Virus / Malware

Denial of Service Attack

Operational Error

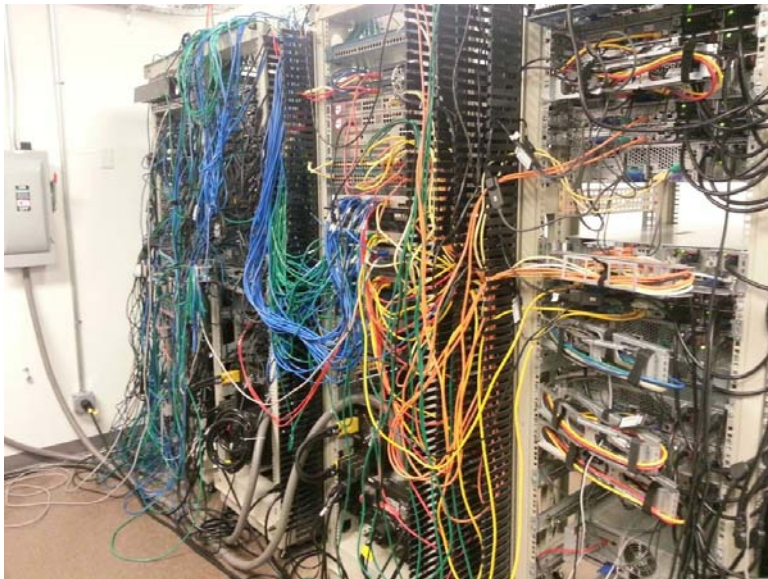
Cyber – How are we exposed ?

Online sales



Cyber – How are we exposed ?

Internal network downtime – not simply a case of logging in remotely

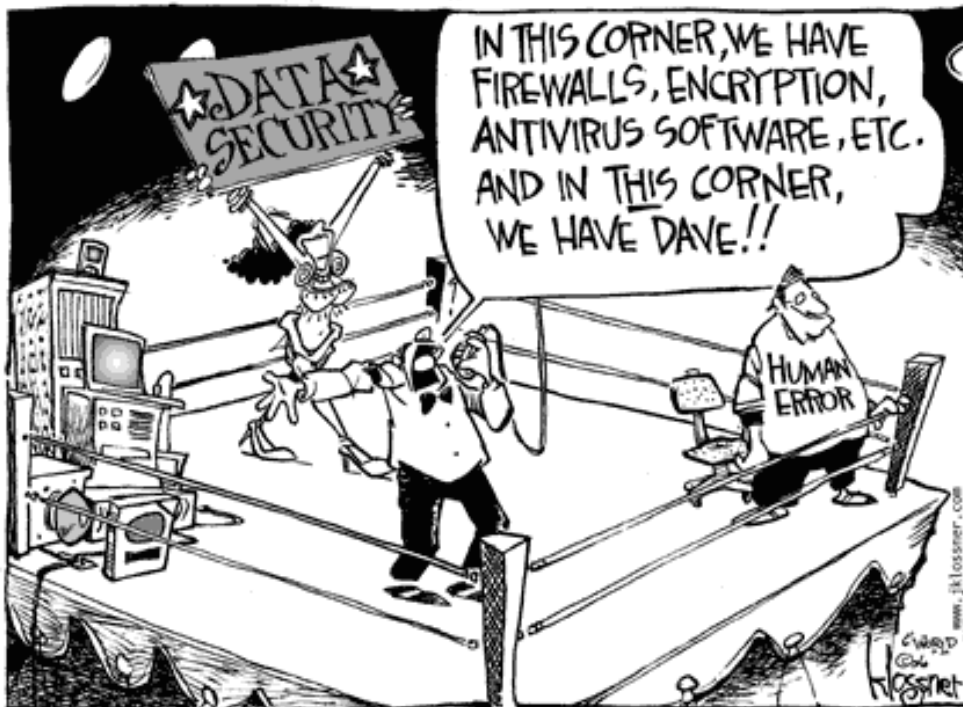


Cyber – How are we exposed ?

Using a data centre doesn't necessarily remove risk



Cyber – How are we exposed ?



**‘We’ are still the
highest risk – social
engineering /
employee errors.**

**7 out of 10 people
arrested for cyber
crime were employees**

Cyber – How are we exposed ?

Example 1 – A phishing emailⁱⁱⁱ Although it appears to be from O2, closer inspection, by right clicking or hovering over the name, shows the email address has been spoofed. For example, 'user123@o2-mail.com'. An official O2 email would come from '@o2.co.uk'.

This message was sent with High importance.

From: O2Billing
To: [redacted]@o2.co.uk
Cc: [redacted]
Subject: Your O2 bill is ready #1035346

The subject title is O2 (zero-two) not O2

Dear Customer

It is addressed generically, not to the customer by name

Your O2 bill for 28/05/14 is now ready. You can [look at your bill here](#).

In total, your bill for this month comes to £372,85. We'll request this amount from your chosen account on, or just after, the date in your bill.

To see your bill, you'll need the username and password you were given when you joined O2. If you've forgotten them, we can give you a [reminder](#).

Is your bill more than you were expecting?
If so, here's a few reasons why this might be:

- You could have gone over the minutes, texts or data that's in your allowance.
- You could have called or sent texts to numbers that can't be taken from your allowance such as International, 0800, 0845 numbers or directory enquiries.
- You have used your phone for calls, text or data whilst abroad.

Hovering over the link here will show that it will not take the user to O2's website, but to a completely unrelated website

To view any charges outside your allowance [click here](#)

A comma is used instead of a decimal point

If you have any questions, just [ask Lucy](#). See our online virtual agent. You can also find out more about what's included in your bill with an [online demonstration](#).

Best regards

O2

By the time this email was sent, O2 has discontinued their 'Lucy' virtual assistant

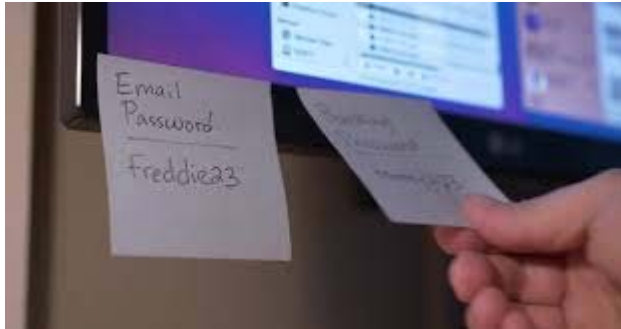
This email is sent from Telefónica UK Limited. Registered office:
260 Bath Road, Slough, Berkshire, SL1 4DX. Registered number: 7270332.
Please do not reply.

Cyber – How are we exposed ?

Telephone networks
– phone hacking or phreaking



Cyber – How are we exposed ?



Are we the weakest link into another network – 75 % of reported breaches traced to a trusted connection. Hackers exploit smaller companies due to weaker security / protection



Cyber – How are we exposed ?

Data protection – encryption is just part of the answer. Paper documents and physical records more widespread

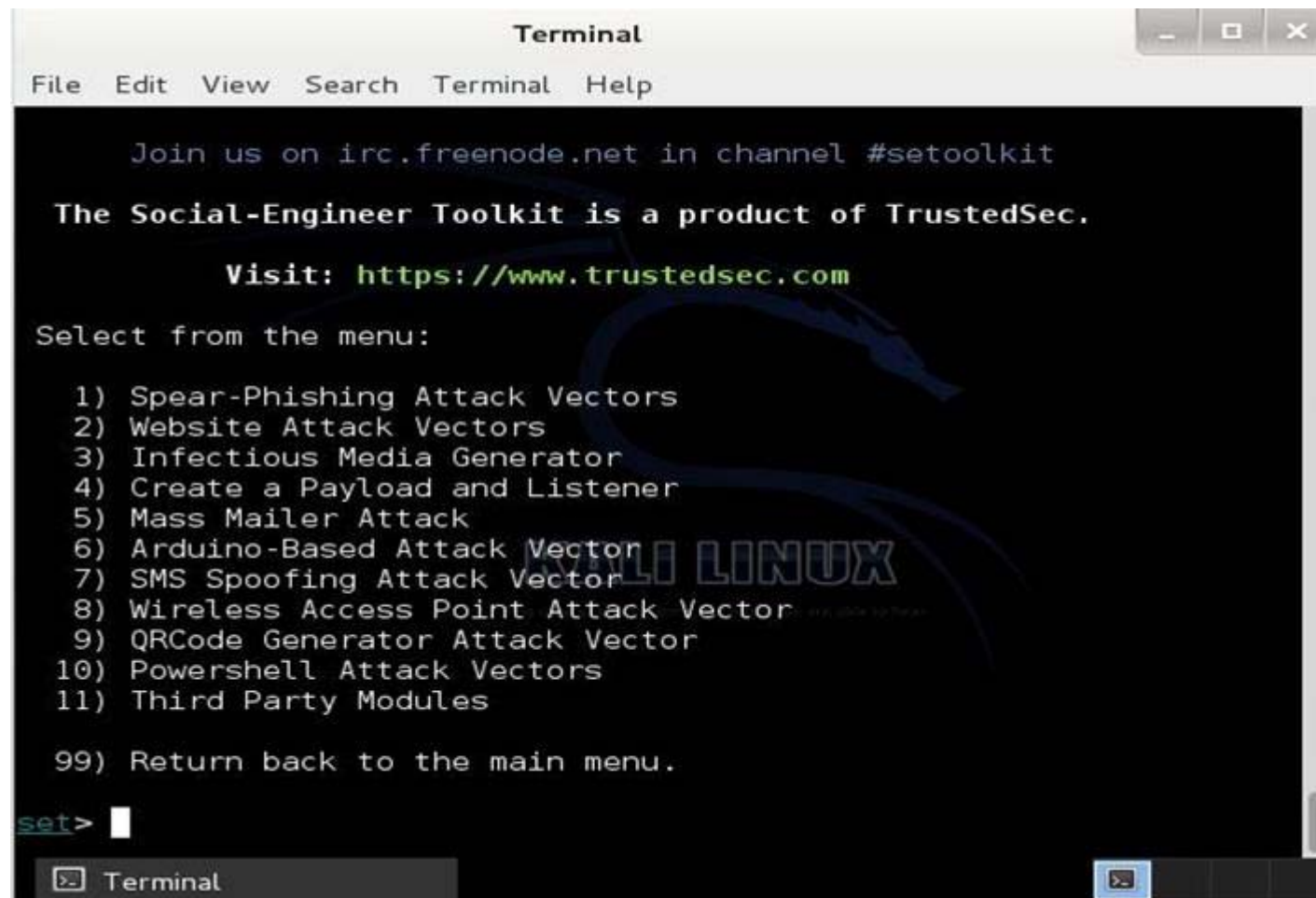


Cyber – How are we exposed ?

Business Interruption losses often larger than data breach costs – 2/3 of DDOS attacks lasted over 6 hours, with 12 % lasting from 1 day to over a week



Cyber – How are we exposed ?



The image shows a terminal window titled "Terminal" with a menu for the Social-Engineer Toolkit (SET). The menu lists various attack vectors and modules. A watermark for "KALI LINUX" is visible in the background of the terminal.

```
Terminal
File Edit View Search Terminal Help

Join us on irc.freenode.net in channel #setoolkit

The Social-Engineer Toolkit is a product of TrustedSec.

Visit: https://www.trustedsec.com

Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) SMS Spoofing Attack Vector
8) Wireless Access Point Attack Vector
9) QRCode Generator Attack Vector
10) Powershell Attack Vectors
11) Third Party Modules

99) Return back to the main menu.

set> 
```


Cyber – How are we exposed ?

IT expertise and size of teams



Cyber – How are we exposed ?

31 % of cyber attacks / incidents from inside the organisation



Cyber - Coverages

Liability Sections

Defence Costs, Damages & Regulator Fines

Damage to Third Party Networks & Data / Failure of Security

Failure to protect/wrongful disclosure of information (including employee information)

Privacy or Security related regulator investigation

As above when committed by a third party you outsource to (e.g. Cloud Provider)

Media content infringement / libel / slander / defamation

First Party Sections

Insured's Loss

Network Restoration

Business Interruption and Extra Expense

Data Restoration

Cyber Theft

Cyber Extortion

Telephone Hacking

Adulteration of Stock

Expense/Services

Expenses Paid to Third Party Providers

Privacy Breach Notification Costs

Forensic Investigation Costs

Credit Monitoring

Privacy Breach Legal Advice

PR Costs

Cyber – Social Engineering / Impersonation Fraud

Impersonation Fraud is a scheme that involves an imposter requesting a fraudulent payment.

The perpetrator usually assumes the identity of an authority figure to request a payment to another party (Chairman / Financial Director or vendors).

Delivery method could be email, text or even a phone call

The request is usually for a bank transfer in order to secure immediate transfer of funds.

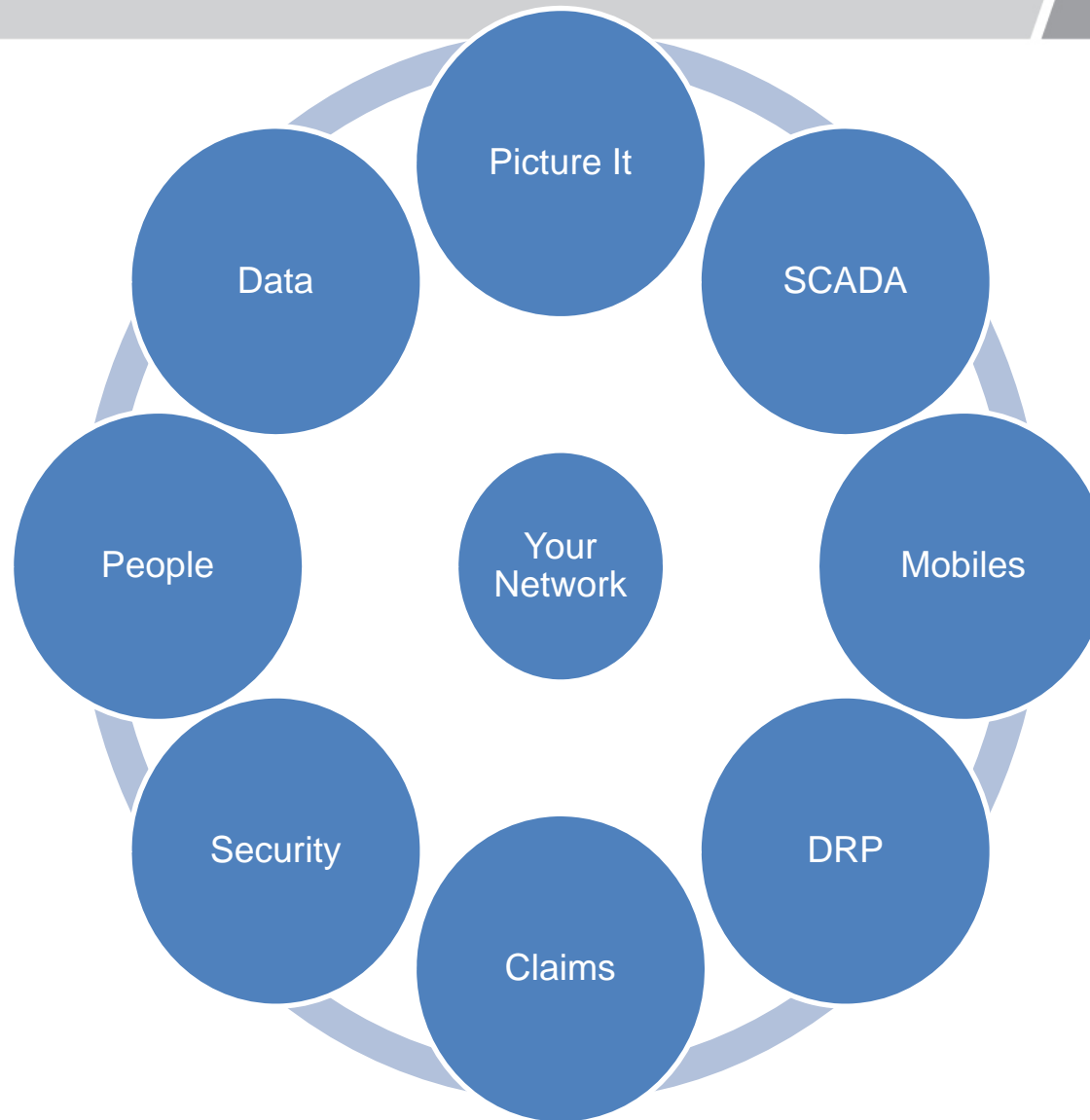
Cyber – GDPR Fines

Under new regime, there is a two-tiered sanction regime.

Lesser incidents will be subject to a maximum fine of either €10m or 2% of an organisation's global turnover (whichever is greater)

While the most serious violations could result in fines of up to €20m or 4% of turnover (whichever is greater).

Cyber – Risk Features



Cyber – Merits of a Cyber Breach Partner

Conflict of interest with the current IT provider – uncover the truth !

Speed of response – the first hours are vital

Cost – contacting a forensic consultant etc when all ‘hits the fan’—thousands!

Experience – keeping the message relevant and clear by removing emotion



Cyber – Real Claims Examples



“Unhappy (former) IT Director encrypts customer database”.

Cyber – Real Claims Examples



“Law firm – unaware of ongoing hacking event”

Cyber – Real Claims Examples



Insurance brokers.....

Cyber



Questions / Comments / Experiences !