Data Disasters and How To Prevent Them

Thursday 9 June 2022

Presenters

Kate Burt | Head of Risk & Compliance | Legl

Kate qualified as a solicitor in 2007 and spent more than a decade as a litigator before finding her niche in law firm risk and compliance in 2016. She now advises law firms and RegTech providers nationally in relation to their regulatory obligations with a particular interest in tech innovation. Kate's work focuses on due diligence and regulatory aspects relating to law firm PII, merger & acquisition, changing legal entity applications and new law firm start-ups.

Louise Gibson | Detective Sergeant | Leicestershire Police

Louise has been a Police Detective since 2010 and has specialised in cybercrime since 2017. Louise is trained in computer network security and has completed a MSc in cybercrime. Louise is also a keen ethical hacker and part of her work is mentoring young adults into positive employment within cyber security.

David Gilmore | Director and Founder | DG Legal

David founded DG Legal in 2000. He has worked with several government departments and has advised dozens of charities involved in the legal. David has also provided advice and assistance to hundreds of law firms and other legal organisations. He delivers specialist consultancy and training on a wide range of topics including business management & strategy, tendering, compliance and quality assurance.

Presenters

Nick Hanning | Consultant | DG Legal

Nick has a wealth of legal practice, practice management and regulatory experience. He is a Fellow of the Chartered Institute of Legal Executives (CILEx) and served as CILEx President in 2012-13. He has developed expertise in Data Protection Law. He is a Data Protection Officer and regularly advises DG Legal's retainer clients and others about the GDPR and Data Protection Act issues.

Matt Howgate | Consultant | DG Legal

Matt is a non-practising solicitor and was formerly Senior Legal Adviser and Head of Continuous Improvement at the Legal Services Commission. He has considerable experience in regulatory issues and advising on complex issues of compliance and ethics. He is also an expert in data protection, GDPR and on the civil legal aid scheme.

Adam Makepeace | Consultant | DG Legal

Adam is a qualified solicitor and holds an MBA. He was involved in legal practice management for more than 15 years, including 12 years managing respectively the largest civil legal aid firm and the largest criminal legal aid firm. In 2018, Adam won both the inaugural LAPG award for Practice Manager of the Year, as well as the award for Access to Justice through IT.

Agenda

- Introduction
- The true cost of cyberattacks to law firms
- Current cyber threats and how to protect yourself
- Case Study: Tuckers Solicitors Ransomware Attack
- What firms can do to prevent data breaches and protect their clients
- Panel discussion on data/cyber security
- Q&A and closing

The True Cost Of Cyberattacks To Law Firms

David Gilmore | Director and Founder | DG Legal

39% of UK businesses identified a cyber attack in 2021/22 according to the Government

https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022

75% of law firms visited by the SRA in 2020 for a thematic review had been the target of a cyber attack

https://www.sra.org.uk/sra/research-publications/cyber-security/

Why are law firms targeted?

- High value transactional work
- Perception that many law firms are not tech savvy
- Handling of very sensitive client information
- Representing unpopular clients of firms in controversial territories

Most common methods that cybercriminals use

- email modification
- spyware
- ransomware
- viruses
- denial of service attacks
- gaining remote access to a firm's systems

https://www.sra.org.uk/sra/research-publications/cyber-security/

The true cost of cyberattacks for law firms

- Direct financial loss
- Indirect financial loss
- Fines and penalties
- Reputational loss
- Data loss
- Stress

Current Cyber Threats And How To Protect Yourself

Louise Gibson | Detective Sergeant | Leicestershire Police

Legl

DGLEGAL
Services for Lawyers

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Cyber Awareness

In an emergency call **999**

For non emergencies call **101**

@EMCyberSecure

www.eastmidlandscybersecure.co.uk

LEICESTERSHIRE POLICE

What are the current threats to businesses?

National Cyber Security Centre
a part of GCHQ

Cyber Aware

- Phishing
- Ransomware

Phishing

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Phishing is a type of social engineering where attackers influence users to disclose information or click a bad link.

Phishing is commonly carried out via email, text and phone calls.

Don’t click on the links or attachments in suspicious emails, and never respond to messages that ask you or your personal or financial details.

Phishing attempts can be reported to **report@phishing.gov.uk** for emails.
Report text scams by forwarding message to 7726.

Tell Tale Signs of Phishing

National Cyber Security Centre
a part of GCHQ

Cyber Aware

How is it addressed to you?

Threat to act urgently?

Are logo's/ graphics quality as expected?

Does it sound legitimate, or is it trying to mimic someone you know?

Addressed by Bank or Authority?

If it sounds too good to be true, it probably is.

Scale of Ransomware

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Ransomware attacks are increasing globally and is the NCSC's number one focus.

47% of UK Businesses have been affected by ransomware attacks.

73% of organisations surveyed reported that the cybercriminal had succeeded in encrypting the data.

Ransomware is the biggest cyber threat to businesses.

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Common Attack Methods

Ransomware can infect your network in a number of ways:

1. Phishing emails
2. Remote Desktop Protocol (RDP)
3. Access bought on criminal market places
4. Zero-day exploits

If You Are Infected:

National Cyber Security Centre
a part of GCHQ

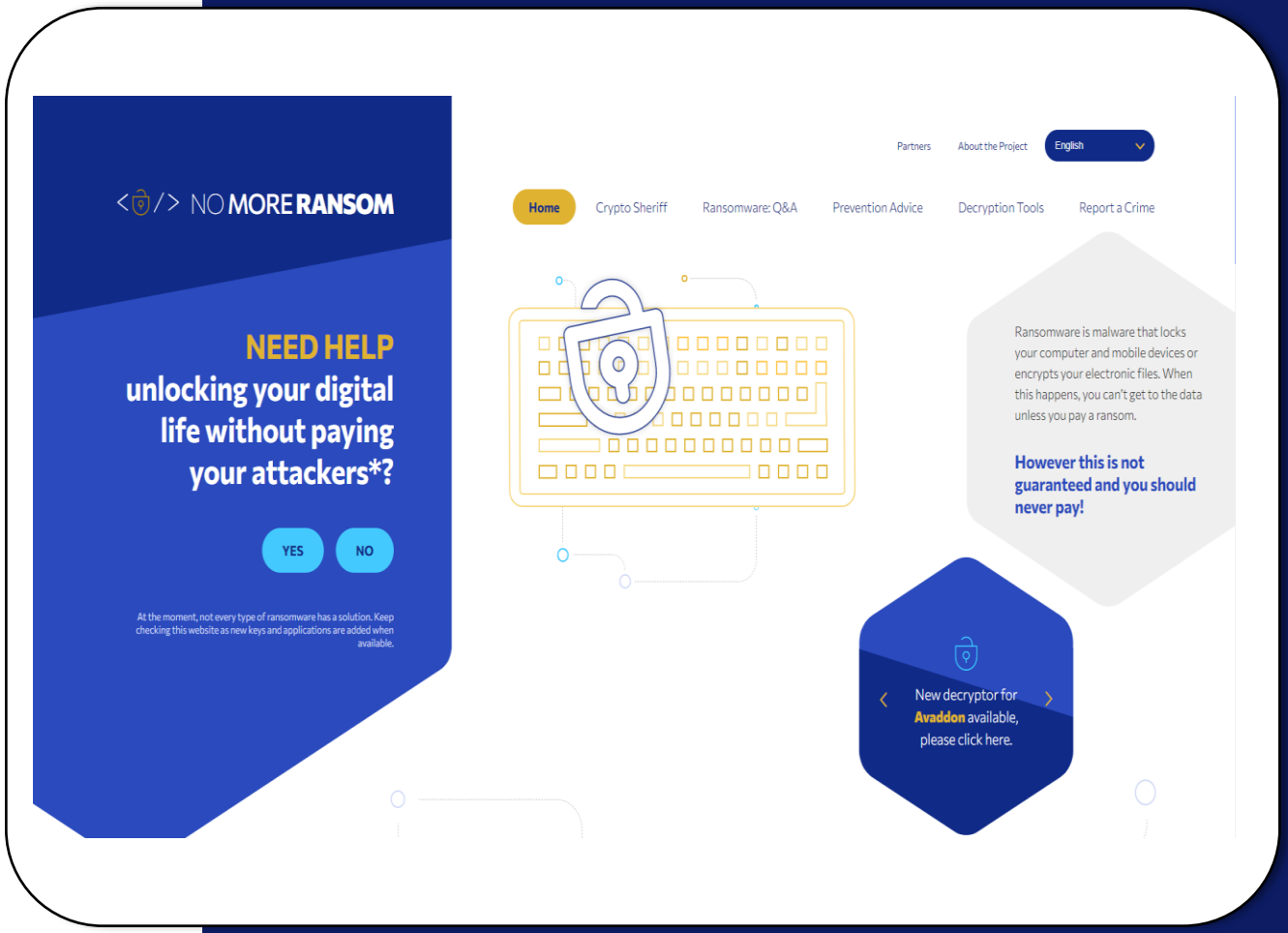
Cyber Aware

- We advise you to not pay the ransom
- Disconnect any infected devices from the wider network as it may compromise other devices
- Change passwords that are mentioned
- Check if other accounts have been compromised
- Ensure your backup is free from malware when you are restoring your data/ network

National Cyber Security Centre
a part of GCHQ

Cyber Aware

Check if you have fallen victim to Ransomware.



www.nomoreransom.org

@EMCyberSecure

Services We Offer:

National Cyber Security Centre
a part of GCHQ

NCA
National Crime Agency

Offer Victim Support/ Engaging with those on cusp of cyber criminality

Cyber Security Reviews & support for Cyber Security standards

Table Top Exercises/Staff Awareness Training

General Advice Guidance and Awareness at events

Thank you! – Any Questions?

National Cyber Security Centre
a part of GCHQ

Cyber Aware

More information

- https://www.ncsc.gov.uk/collection/small-business-guide

- Get in touch
  - Cyber Security Engagement Team
  - EMSOUcyberprotect@leicestershire.pnn.police.uk

https://www.smartsurvey.co.uk/s/EMSOU2122BUS/

Business Survey
21.22

Case Study: Tuckers Solicitors Ransomware Attack

Adam Makepeace | Consultant | DG Legal

My Case Study is about this…

The Law Society Gazette

Cont

NEWS | ANALYSIS | LAW | PRACTICE | IN-HOUSE | PEOPLE | JOBS

NEWS

Firm fined almost £100,000 over ransomware attack

By John Hyde | 10 March 2022

8 Comments

Criminal defence firm Tuckers Solicitors has been fined £98,000 after failing to secure sensitive court bundles that were later published on the dark web and held to ransom by organised criminals.

ico. Information Commissioner's Office

The UK's independent authority set
rights in the public interest, promot
bodies and data privacy for individu

Home | Your data matters | For organisations | Make a compla

Action we've taken / Enforcement / Tuckers Solicitors LLP mpn

Tuckers Solicitors LLP

Date **10 March 2022**
Type **Monetary penalties**
Sector **Legal**

Tuckers Solicitors LLP contravened Article 5(1)(f) of the GDPR.

Tuckers Solicitors LLP monetary penalty notice

Action we've taken

[Firm fined almost £100,000 over ransomware attack | News | Law Gazette]

One morning…I was here…

…with these guys

…then

25/8/2020 – 05.23am

Morning Adam – I think that we have been victims of a Cyber attack

Chirag

…then

25/8/2020 – 05.36am

What makes you say that?

Adam

…then

25/8/2020 – 05.38am

No emails are working and I have just connected remotely to my machine in the Warren Street office and there is a notice on the desktop which says “you have been cyber attacked – give us all your money to release your data”

Chirag

Note: it said something like that! I have not got the message anymore!

Things that aren’t in your BCP…

- Data connectivity is rubbish in Hampshire
- The only wifi in Hampshire is in Starbucks/pubs
- Parking meters in Hampshire don’t use Ringo/Pay by Phone etc
- Shop keepers in Hampshire are really grumpy when you ask if they will give you change for the parking meter

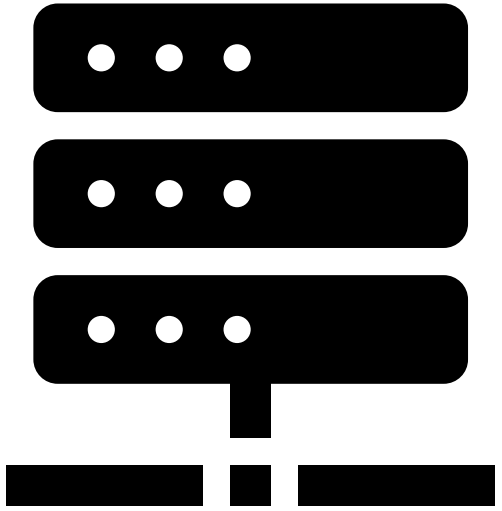
But eventually you can get plugged in and start to organise your response…

What do you have to do…

1. Do the basic reporting;
   - ICO
   - SRA
   - NCA
2. Work out which parts of the business you need to get up and running again – and how!
3. Deal with the Cyber criminals – if necessary

So – what did they do? We had…

- Case Management System; including
  - all Accounts
  - Documents on live and archived cases



- Legacy servers behind a Citrix gateway which had
  - Our old File Server
  - MS Exchange Server

They attacked the legacy system…

33. On 27 August 2020 Tuckers commissioned third-party investigators, [redacted], to provide a 'Cyber Security Incident Response Report'. Neither Tuckers nor [redacted] was able to determine conclusively how the attacker was able to access Tuckers' network. However, it did find evidence of a known system vulnerability [redacted] that could have been used to either access the network, or further exploit areas of Tuckers once inside the network.

34. [redacted] released a patch for [redacted] in January 2020. Tuckers has told the Commissioner that it applied the patch in June 2020, but it has accepted that the attacker could have exploited it during the five-month unpatched period[3].

They weren't targeting "us"…

Maze, a notorious ransomware group, says it's shutting down | TechCrunch - November 2020

One of the most active and notorious data-stealing ransomware groups, Maze, says it is "officially closed."

The announcement came as a waffling statement, riddled with spelling mistakes and published on its website on the dark web, which for the past year has published vast troves of stolen internal documents and files from the companies it targeted, including Cognizant, cybersecurity insurance firm Chubb, pharmaceutical giant ExecuPharm, Tesla and SpaceX parts supplier Visser and defense contractor Kimchuk.

"Obviously, Maze's claims should be taken with a very, very small pinch of salt," said Brett Callow, a ransomware expert and threat analyst at security firm Emsisoft. "It's certainly possible that the group feels they have made enough money to be able to close shop and sail off into the sunset. However, it's also possible — and probably more likely — that they've decided to rebrand."

Once they were inside – they could do whatever they wanted!

35. Once inside the network, the attacker installed various attacker tools which allowed the attacker to create its own user account, which it did. The attacker used this account to execute the attack and encrypt a significant volume of personal data contained in case bundles held on the archive server within the Tuckers network (see paragraph 29 above). As well as encrypting the personal data and the backups, the attacker also exfiltrated 60 court bundles and released them onto the dark web.

They encrypted thousands of files – and extracted around 60 folders

29. In total, 972,191 individual files were encrypted. Of these, 24,711 related to court bundles. Of the 24,711 court bundles, 60 were exfiltrated by the attacker and published on an underground market site (the "dark web").

What it doesn't say is that they locked our email accounts – and that is what was really causing issues!

But, boy, was that NOT the end of all the hard work…

- SRA decided that they weren't particularly interested – although that may have changed now that the ICO have published their report
- ICO wanted a forensic amount of information – and initially made noises to the effect that this wasn't the sort of thing where an organisation would normally be fined! We were the victims of a crime!
- ICO also wanted chapter and verse on who and how we were informing of the attack, including (most importantly) the 60 clients to which the data related

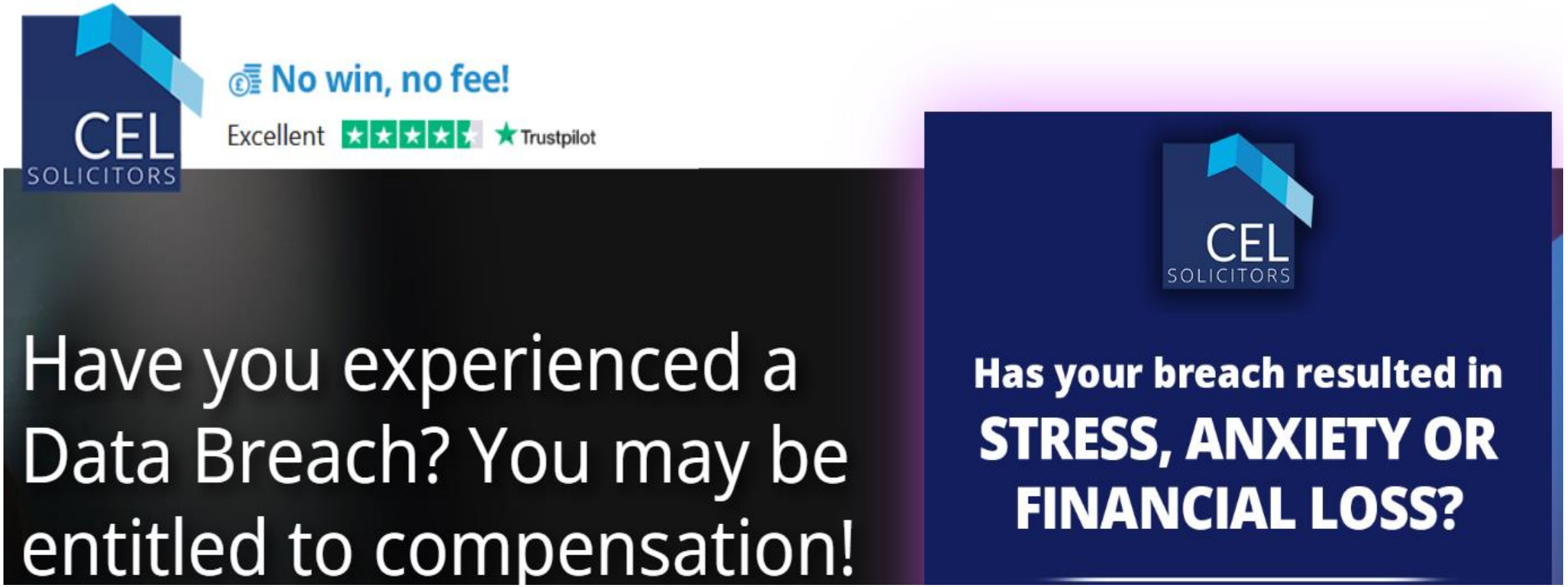
You might not want to tell people – but it would have been worse if we hadn't!

36. Tuckers notified all but seven of the parties detailed within the 60 court bundles which had been released[4]; this was done in line with the requirements of Article 34 GDPR. It also made a public notification of the incident using its social media presence and its website.

Isn’t it ironic…

- But for having to tell people – no-one would ever have known!
- Genuinely believe that no-one has ever accessed the data that was released by the hackers.
- You would have to either
  - know (which is pretty much a direct consequence of us having to publicise everything!); or
  - Be a random “criminal” that wanted to find some angle
- You would need to download the Tor browser
- Navigate to the hackers website
- Search (or browse) through data from (literally) hundreds of random organisations!

I hate ambulance chasers…



Note: I can't remember whether CEL were specifically one of the firms that we heard from, but it was from this ***kind*** of firm.

Other things we did next…

Cyber Griffin

Don’t forget – we had already

- Moved to a different network (mostly before the attack)
- Which had the security required
- We already trained people routinely on cyber security

But

- We enrolled every member of staff on a Cyber Griffin cyber security course
- But, but, but…you can never do enough!

My reflections…

The Contravention

39. For the reasons set out below, and having carefully considered Tuckers' representations, the Commissioner has concluded that Tuckers contravened Article 5(1)(f) GDPR. The Commissioner makes clear that he accepts that primary culpability for this incident rests with the attacker. But for the attacker's criminal actions, regardless of the state of the security, the breach would not have occurred. However, the infringements

We were the victims of a crime.

We need to understand the standards by which we are being judged…

40. In reaching those conclusions, the Commissioner has given consideration to Article 32 GDPR, which requires a controller when implementing appropriate security measures to consider "*the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons*".

These are all "conceptual" issues. (I still believe)

NO-ONE saw the data that was stolen!

So, what are those standards…

41. As part of his deliberations, the Commissioner has considered, in the context of "state of the art", relevant industry standards of good practice including the ISO27000 series, the National Institutes of Standards and Technology ("NIST"), the various guidance from the ICO itself, the National Cyber Security Centre ("NCSC"), the Solicitors Regulatory Authority ("SRA"), Lexcel and 'NCSC Cyber Essentials'.

42. The Commissioner has concluded that there are a number of areas in which Tuckers has failed to comply with, and to demonstrate that it complied with, Article 5(1)(f) GDPR. Tuckers' technical and organisational measures areas were, over the relevant period, inadequate in the following particular respects:

MFA

46. The Commissioner understands that [redacted] published guidance in 2016 which stated that organisations should not use single factor authentication for [redacted] in production environments. The NCSC has recommended since 2018 to use MFA for services such as remote access. It says that MFA is particularly important for authentication to services that hold sensitive or private data. The NCSC Cyber Essentials requires multi-factor authentication where it is available, and the SRA also published guidance in 2018 which recommended the use of MFA where possible.

47. The Commissioner believes that the use of MFA was a comparably low-cost preventative measure which Tuckers should have implemented, with there being a number of both open and proprietary/commercial MFA solutions widely available that are compatible with[redacted].

Patch immediately!

52. With regards to "state of the art", it is apparent that [redacted] had announced on 17 December 2019 that it was aware of the vulnerability CVE-[redacted] and provided mitigation steps to prevent exploitation of it, with a patch to fix the vulnerability being released on 19 January 2020. At the time of becoming aware of the vulnerability, [redacted] advised in a published security bulletin on its website that it "*strongly urges affected customers to immediately upgrade to a fixed build OR apply the provided mitigation which applies equally to* [redacted] *and* [redacted] [redacted] *deployments*".

Data encryption

- **Failure to encrypt personal data**

64. With regards to "state of the art", The Commissioner has taken into consideration relevant standard of best practice, including the ISO27001 requirement to implement cryptographic controls in compliance with all relevant agreements, legislation and regulation. NIST 800-53 also discusses how the selection of cryptographic mechanisms should be based on the need to protect the confidentiality and integrity of organisational information. It says that the strength of a mechanism should be commensurate with the security category or classification of the information. The Commissioner understands that the Tuckers GDPR and Data Protection Policy identified client data as its most sensitive data, requiring the highest level of protection.

Cyber Essentials – this is not a sales pitch – BUT!

85. In addition, Tuckers were accredited by the Law Society's Lexcel Legal Practise Quality Mark. Its March 2018 Standards stated that law practises should be accredited against Cyber Essentials. This further reinforced the conclusion that Tuckers should have had the requisite measures in place to achieve accreditation by at least October 2019, and when it failed its Cyber Essentials assessment, it should have quickly and promptly resolved the inadequacies. Had it done so, it could have demonstrated a

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

Cyber Essentials is suitable for all organisations, of any size, in any sector.

From 1 October 2014, Government requires all suppliers bidding for contracts involving the handling of certain sensitive and personal information to be certified against the Cyber Essentials scheme.

The fact we are regulated was an "aggravating factor"

106. The Commissioner has considered the following **aggravating factor** in this case:

The SRA has a published 'Code of Conduct for Firms'. Of particular relevance here are the requirements to: [Para 2.1(a)]

"*Have effective governance structures, arrangements, systems*

The Commissioner considers that Tuckers has failed to meet these standards of the Code.

There were 13 listed mitigating factors – too many to copy here!

107. The Commissioner has considered the following **mitigating factors** in this case:

- Tuckers has proactively sought to address the security concerns and engaged with third party experts to increase the security of its systems, including

And the upshot was…

120. Taking into account all of the factors set out above, the Commissioner has decided to impose a penalty on Tuckers of **£98,000** (**ninety-eight thousand pounds**).

Questions?

Any questions after all that…?

What Firms Can Do To Prevent Data Breaches And Protect Their Clients

Kate Burt | Head of Risk & Compliance | Legl

What Firms Can Do To Prevent Data Breaches and Protect Their Clients

Kate Burt

Solicitor, experienced compliance consultant and Head of Risk & Compliance for Legl

Over 20 years' experience in the legal sector, qualified as a solicitor in 2007. Practiced as a litigator in 3 of the top 50 law firms before finding her niche in law firm risk and compliance in 2016.

Advises law firms nationally in relation to their regulatory obligations and supports Legl with their award-winning client lifecycle management platform providing industry insights and subject matter expertise.

Legl

Overview

- SRA Cyber Report
- Common personal data breaches
- Key areas of data security
- Establishing a culture of privacy

SRA **Risk Outlook Report**

Regarding information security and cybercrime:

- Phishing and email modification make up half of all cybercrime reported to SRA
- Conveyancing still the main target but this is widening to other work areas
- Voice impersonation systems are being used
- Ransomware (loss of system, sensitive client information)

What is **personal data**?

Personal data only includes information relating to natural persons who:

- can be identified or who are identifiable, directly from the information in question; or
- who can be indirectly identified from that information in combination with other information.

What is a **personal data breach**?

"A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed."

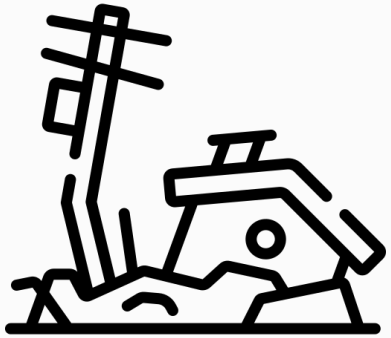
Common **Breaches**

Human Error

Emails to the wrong recipient

Accidentally authorising MFA

Files or laptops left in public places

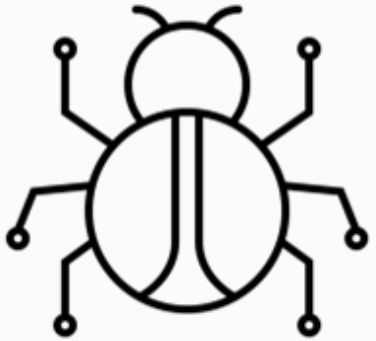


Natural Disaster

Accidental destruction of physical documents

Flood

Fire



Malicious Intent

Cyber attack

Unauthorised access

Legl

Integrity and **Confidentiality (The Security Principle)**

- **Confidentiality**
  Protecting against unauthorised access, distribution or publication.
- **Integrity**
  Protecting against unauthorised modification, corruption or tampering.
- **Availability**
  Protecting against unplanned loss, destruction or unavailability.

Legl

Security **Controls**

Technical

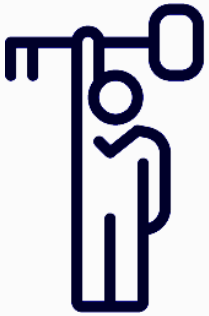
Firewalls, network perimeter defences, anti virus solutions, 2FA, strong passwords

Procedural

Social media policies, data protection policies and procedures, acceptable use policies, data mapping, data breach procedures, recovery plans

Personnel

Pre-employment screening, security awareness training, internal policy training

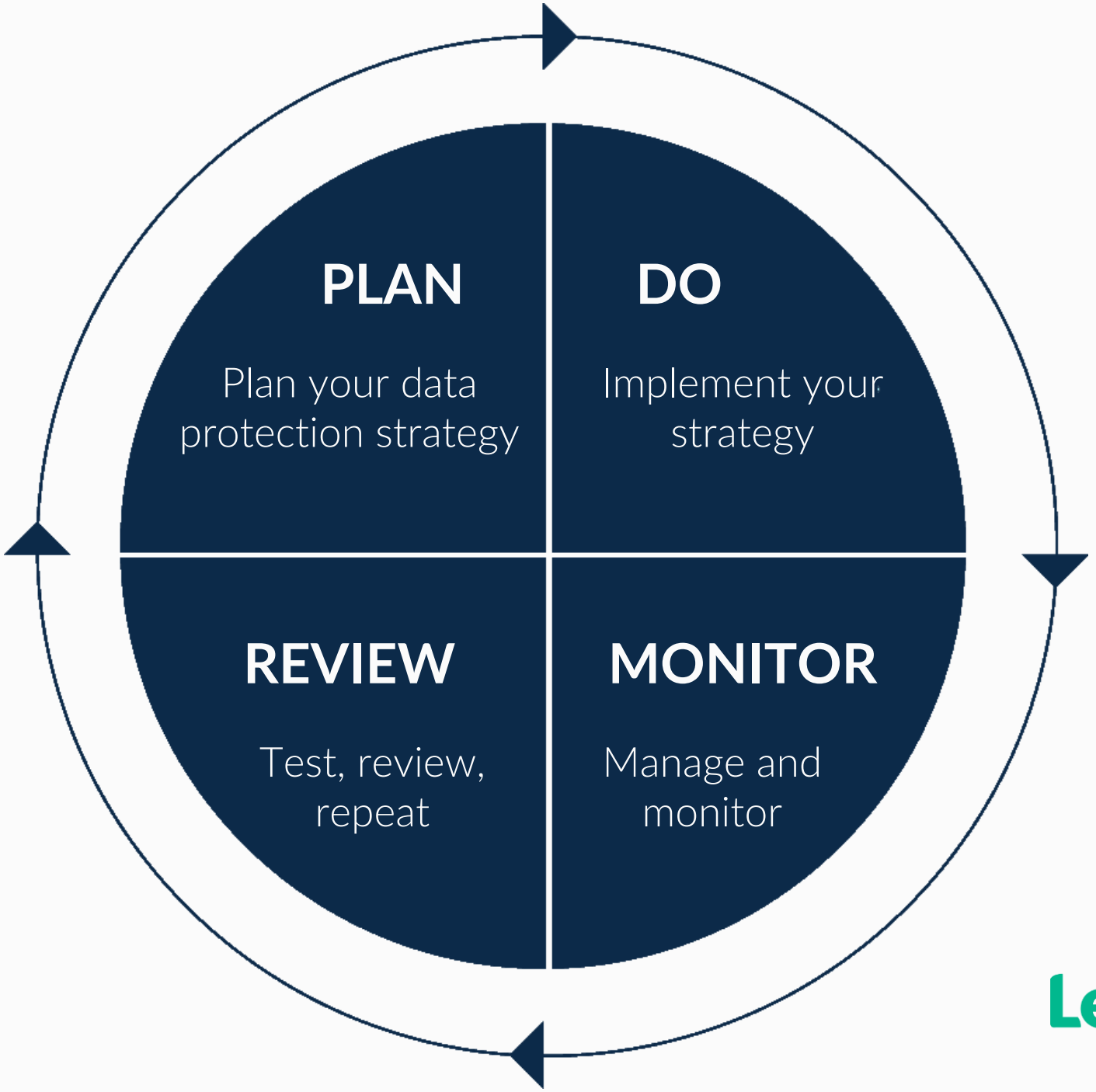


Physical

Lockable filing cabinets, intruder alarms, fire alarms, smoke detectors, security doors, clear/secure desk

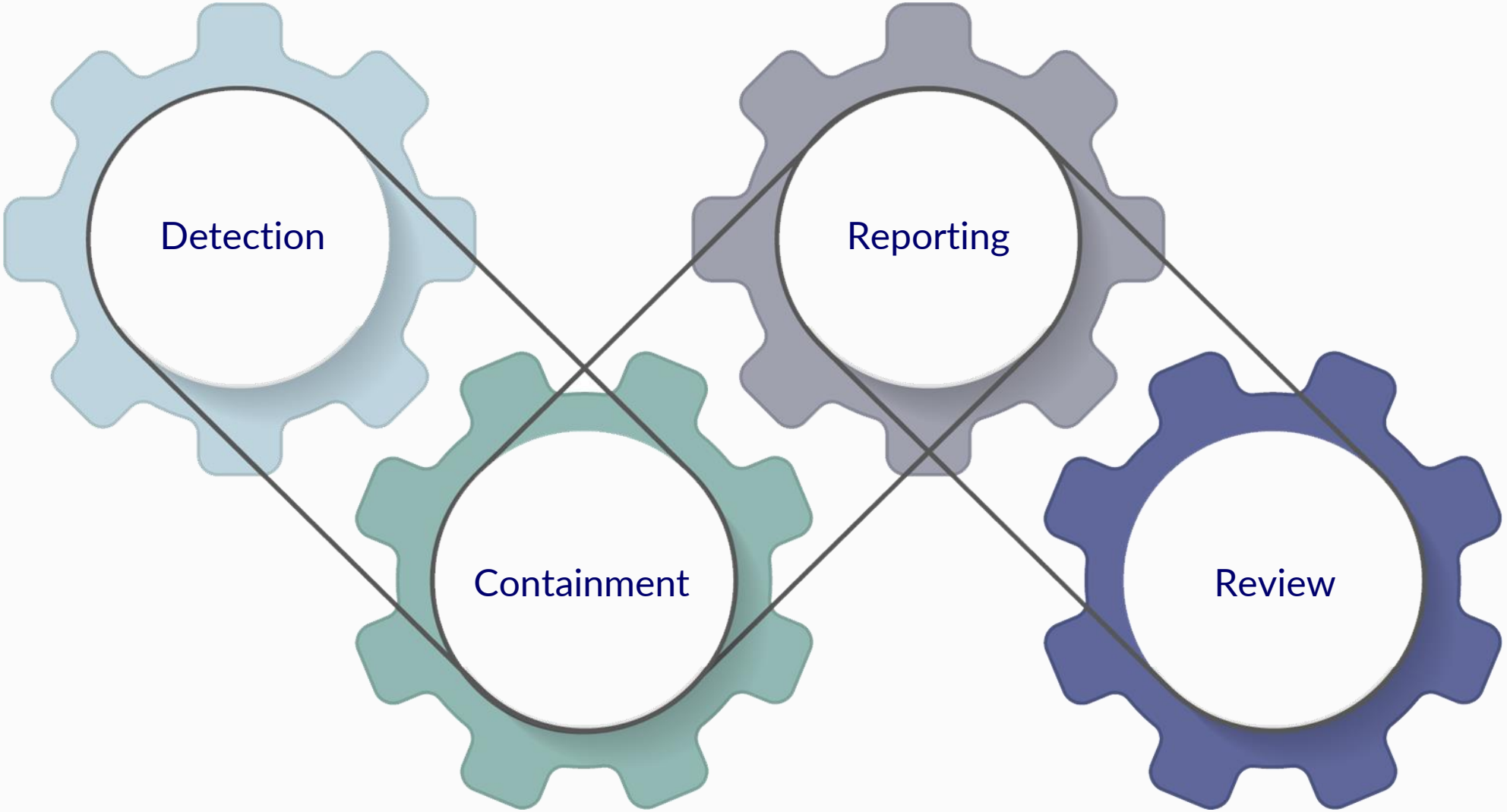
Legl

Prevention is better
than a Cure



Legl

How do you respond to a **breach**?



Legl

Establishing a **Culture of Privacy**

- ✔ Top down (lead by example)
- ✔ Share learnings from near misses and encourage openness
- ✔ Appoint data protection champions
- ✔ Training
- ✔ Reinforce training with regular reminders and examples
- ✔ Consider data security frameworks (ISO27001, Cyber Essentials / Cyber Essentials (Plus), NIST)

Legl

Recommended **Reading**

SRA's Risk Outlook Report: Information Security and Cybercrime in a New Normal

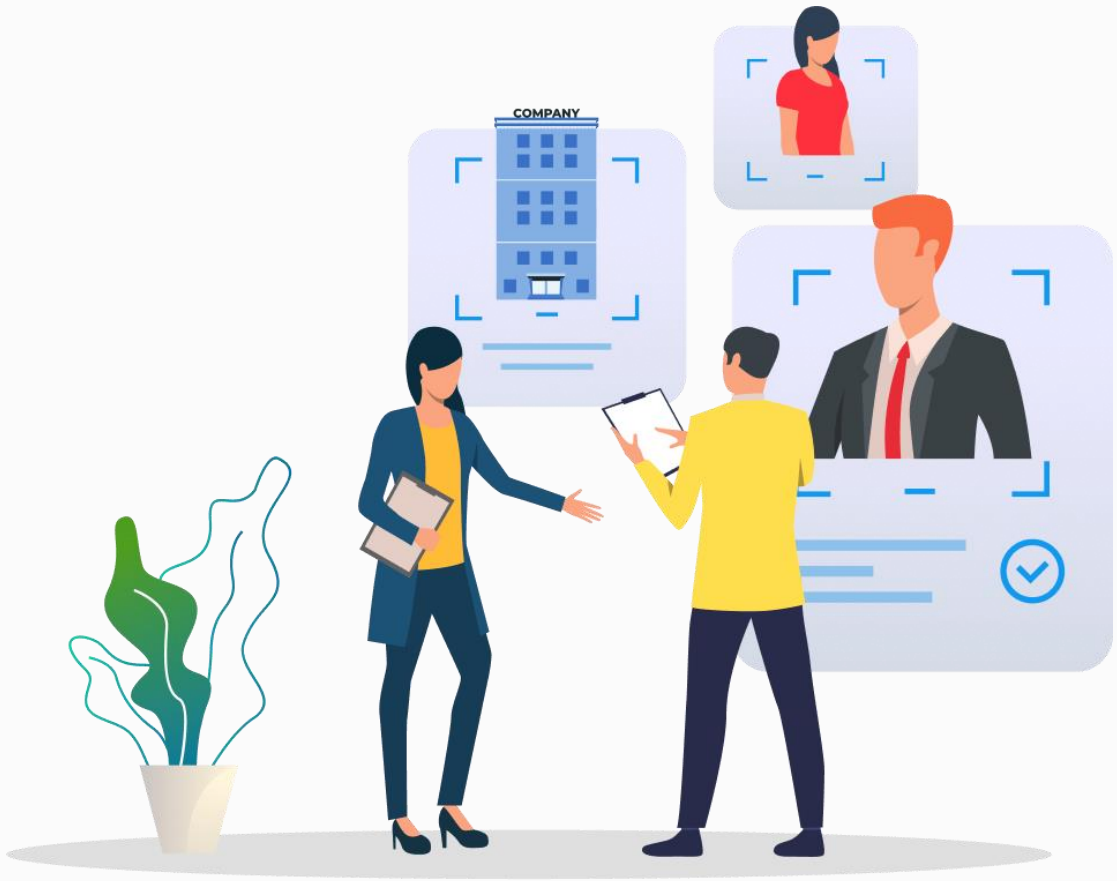
SRA: Information and Cyber Security

ICO's Guide to GDPR

Law Society Guidance on Reporting a Data Breach

Law Society's Cybersecurity News Digest

Howden - Cyber Insurance: A Hard Reset



Thank you!

Legl's award-winning client lifecycle management platform automates client-facing business processes and payments while creating rich data and a single source of truth for law firms.

Visit **www.Legl.com** for more details.

Legl

Panel Discussion

Kate Burt | Head of Risk & Compliance | Legl
Louise Gibson | Detective Sergeant | Leicestershire Police
David Gilmore | Director and Founder | DG Legal
Nick Hanning | Consultant | DG Legal
Matt Howgate | Consultant | DG Legal
Adam Makepeace | Consultant | DG Legal

Legl

DGLEGAL
Services for Lawyers

Contact Details

E: hello@legl.com
W. www.legl.com

T: 01509 214 999
E: admin@dglegal.co.uk
W. www.dglegal.co.uk