# Cybercrime – protecting your firm

Robert Loughlin, Executive Director, SRA
William Wright, Paragon Insurance
James Moss, ICO
Rachel Clements, SRA
NCSC Senior Representative

# Today's session

Solicitors Regulation Authority

- Current risks
- Information security and data protection
- Cyber insurance
- Current trends in reports
- Resources from the NCSC
- Summary and close

# Current risks

- An improving picture
- Data protection
- Report, report, report!

# Cybercrime: panel session

- James Moss, Legal Director, Information Commission's Office
- William Wright, Partner and Director, Paragon Insurance
- Rachel Clements, Regulatory Manager, SRA
- Senior representative, NCSC

# Information Commissioner’s Office

# ICO position on ransomware

- Law enforcement do not encourage, endorse, nor condone the payment of ransom demands. The ICO supports this position.

- You should also consider the terminology within the UK GDPR. It requires you to implement “appropriate measures” to restore the data in the event of a disaster.

- The ICO does not consider the payment of a ransom as an “appropriate measure” to restore personal data.

- Appropriate measures include threat assessments, risk assessments and controls such as offline and segregated backups.

- If you can demonstrate appropriate measures (in accordance with the state of the art, cost and risk of processing), then you will be complying with those aspects of the UK GDPR.

# Ransomware

- If attackers have exfiltrated the personal data, then you have effectively lost control over that data.
- This means individuals have lost the protections and rights provided by the UK GDPR. For example, transparency of processing or subject access rights.
- For this reason, we do not view the payment of the ransom as an effective mitigation measure.

# Ransomware

- If you do decide to pay the ransom to avoid the data being published, you should still presume that the data is compromised and take actions accordingly.

- For example, the attacker may still decide to publish the data, share the data offline with other attack groups or further exploit it for their own gains.

- You still need to consider how you will mitigate the risks to individuals even though you have paid the ransom fee.

# When am I ‘aware’ of a breach?

## Article 29 WP Group Guidelines on Personal Data Breach Notifications

- After first being informed of a potential breach, or when it has itself detected a security incident, the controller may undertake a short period of investigation.
- This is to establish whether or not a breach has in fact occurred.
- During this period of investigation the controller may not be regarded as being “aware”.
- However, it is expected that the initial investigation should begin as soon as possible.
- And establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

# Resources

- ICO and NCSC stand together against ransomware payments being made – Joint statement on ransomware
- Ransomware and data protection compliance – Updated ICO Guidance
- UKGDPR - A.4(12) ‘personal data breach’ means 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

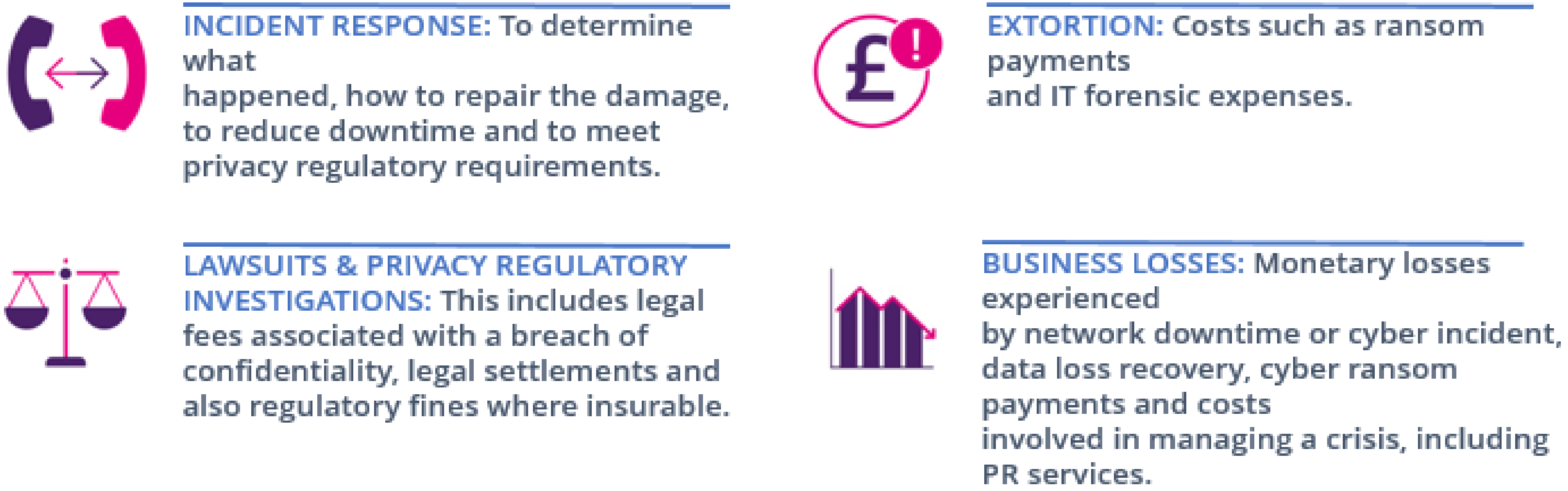
# Cyber Insurance

# Today's Talking Points

- What does cyber insurance cover and what doesn't it cover?
- What controls do cyber insurers look for?
- How are claims handled?
- How can you best manage your cyber risk?

# What is Cyber Insurance?

Insurance for economic or legal costs arising out of DATA DISCLOSURE and/or NETWORK EVENTS:



**INCIDENT RESPONSE:** To determine what happened, how to repair the damage, to reduce downtime and to meet privacy regulatory requirements.

**EXTORTION:** Costs such as ransom payments and IT forensic expenses.

**LAWSUITS & PRIVACY REGULATORY INVESTIGATIONS:** This includes legal fees associated with a breach of confidentiality, legal settlements and also regulatory fines where insurable.

**BUSINESS LOSSES:** Monetary losses experienced by network downtime or cyber incident, data loss recovery, cyber ransom payments and costs involved in managing a crisis, including PR services.

But it is also a crisis management policy not dissimilar to kidnap ransom insurance, in that it offers services as well as financial risk transfer.

# What’s covered?

## Standard parameters of cyber insurance

- Covers liability arising out of a data breach or network security breach or an unintentional act which result in a breach of privacy regulation

- Covers 1st party loss on a named perils basis

# What’s covered?

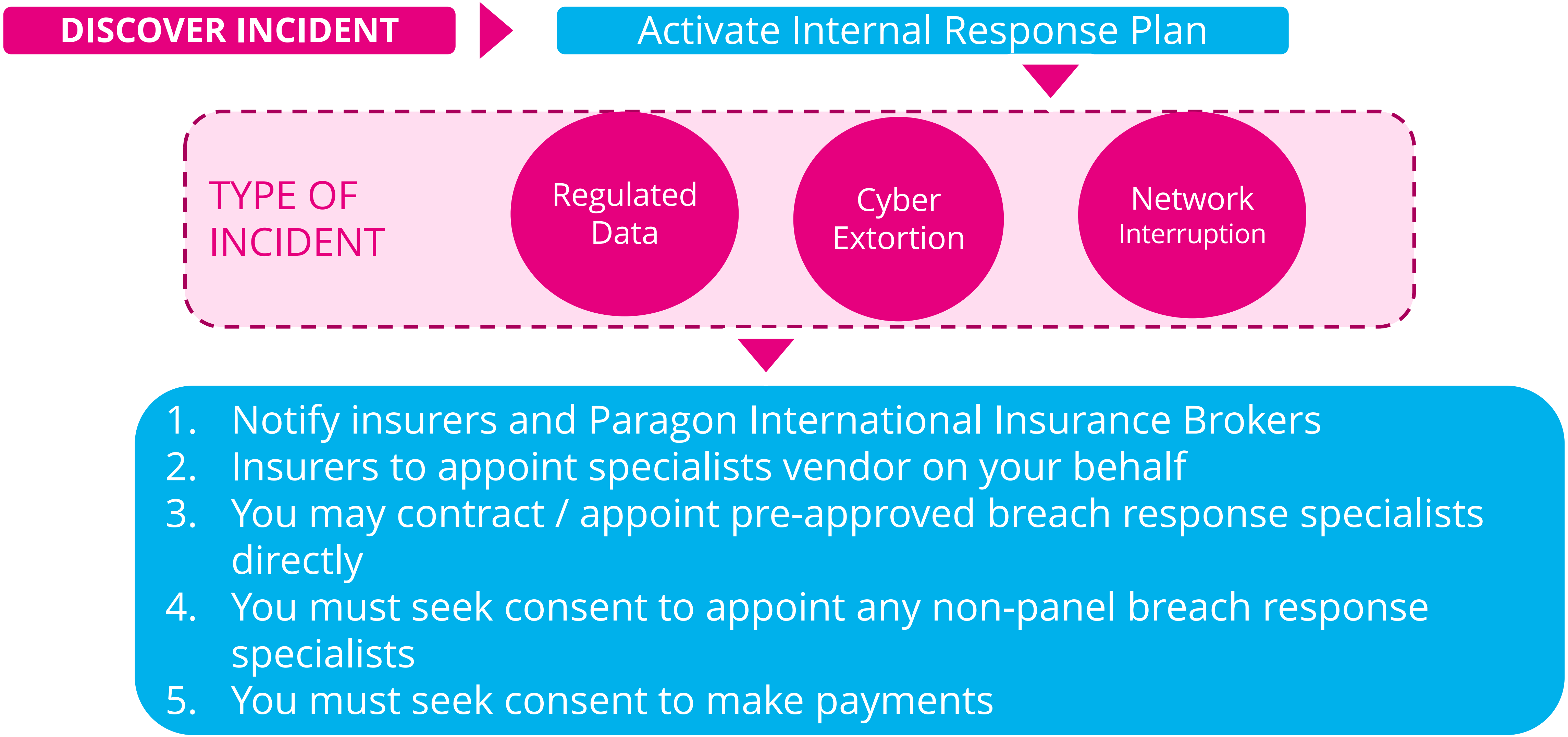
- The asset insured is “data” eg personal records and software etc.
- Money & securities are not “data”  - may also exclude theft of money or securities (refer to Crime policy)
- The network insured (typically) = communications and management information networks

# Incident Response & Insurance

## KEY CYBER RISK CONTROLS

- Encryption
- Multi Factor Authentication
- Training
- Awareness
- Email scanning
- Filtering
- Endpoint Detection
- Intrusion Detection
- Segregated Backups
- Access Control
- Patch Management
- Vulnerability Assessments

# How are Cyber Claims Handled?



DISCOVER INCIDENT

Activate Internal Response Plan

TYPE OF INCIDENT

- Regulated Data
- Cyber Extortion
- Network Interruption

1. Notify insurers and Paragon International Insurance Brokers
2. Insurers to appoint specialists vendor on your behalf
3. You may contract / appoint pre-approved breach response specialists directly
4. You must seek consent to appoint any non-panel breach response specialists
5. You must seek consent to make payments

# How are Cyber Claims Handled?

WHO TO CALL

Data Breach Lawyer [To preserve legal privilege]

Crisis Management Negotiator / IT Specialist

Forensics

Every incident is different, once the initial breach specialist is engaged they will guide you, through the process of incident response

# Remember…

- You can still benefit from the services of the breach response panel, even if you doubt your cyber insurance policy will provide cover for the event

- If the cyber event is covered by your cyber insurance policy, you must notify insurers. If not, you will be required to retrospectively obtain consent by insurers to hire the breach response experts

- This consent will not be guaranteed

# If you want to work with a firm who isn’t approved?

- Your insurer may consider adding your choice of vendor to the panel at your request. Prior approval can ensure fair pricing for vendor services, as opposed to emergency rates

- Provide biographies, showing the requisite skill and experience, as well as the rates they charge showing they are reasonable.

# Risk Management Partners

## HOW CAN YOU BEST MANAGE YOUR CYBER RISK?

Paragon choses 4 partners to evaluate our clients’ security profile and provide risk management services.

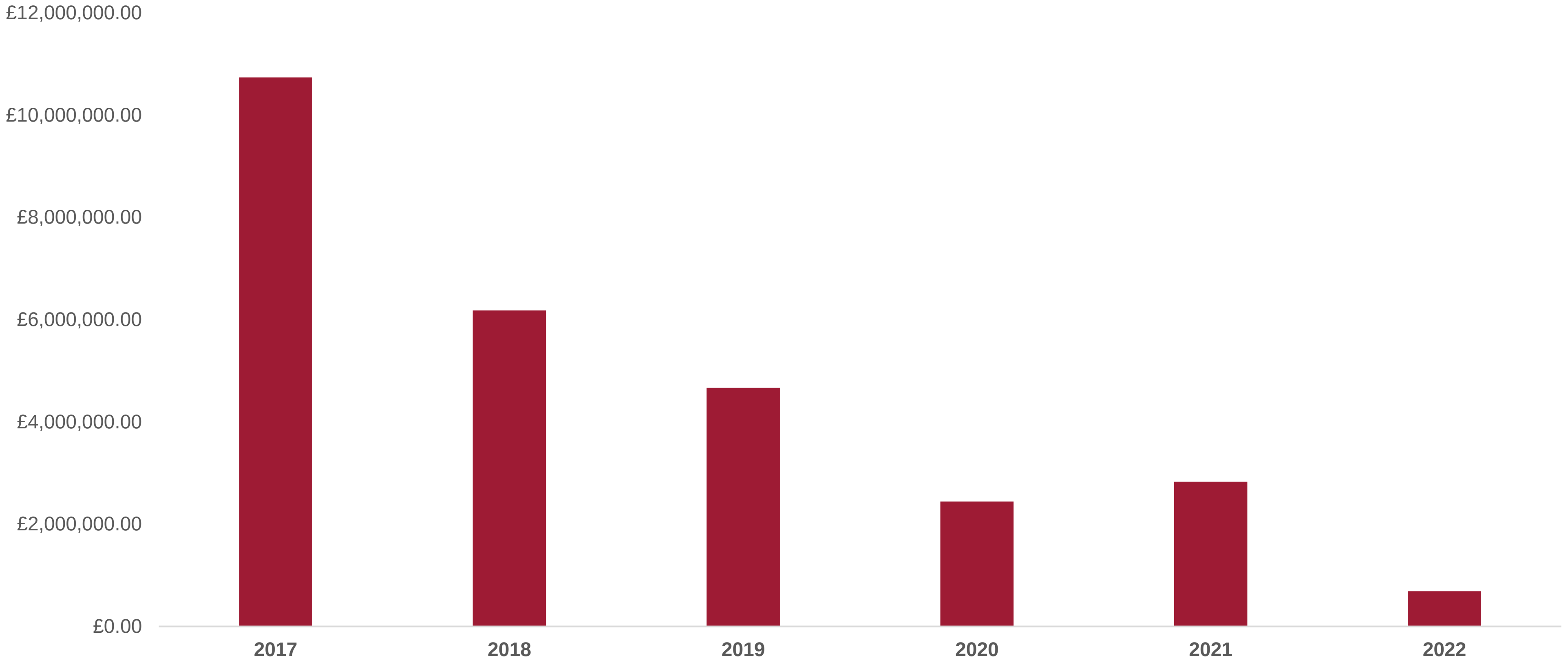
- KYND – Perimeter scanning and external facing security audit, and phishing training tool
- CyberCube – Limit and threat modelling analytics
- BitSight – Third party vendor security monitoring tool
- S-RM – IT Consultancy

KYND CyberCube BITSIGHT S-RM

Paragon

# Current trends: Client losses 2021/22

Solicitors Regulation Authority



# Current trends: Client losses 2021/22

Solicitors Regulation Authority

78% via conveyancing

98% via email modification fraud

9 reports client losses up to Q3 2022

# Reporting an email modification fraud

Solicitors Regulation Authority

report@sra.co.uk

Warning – do not skip this bit

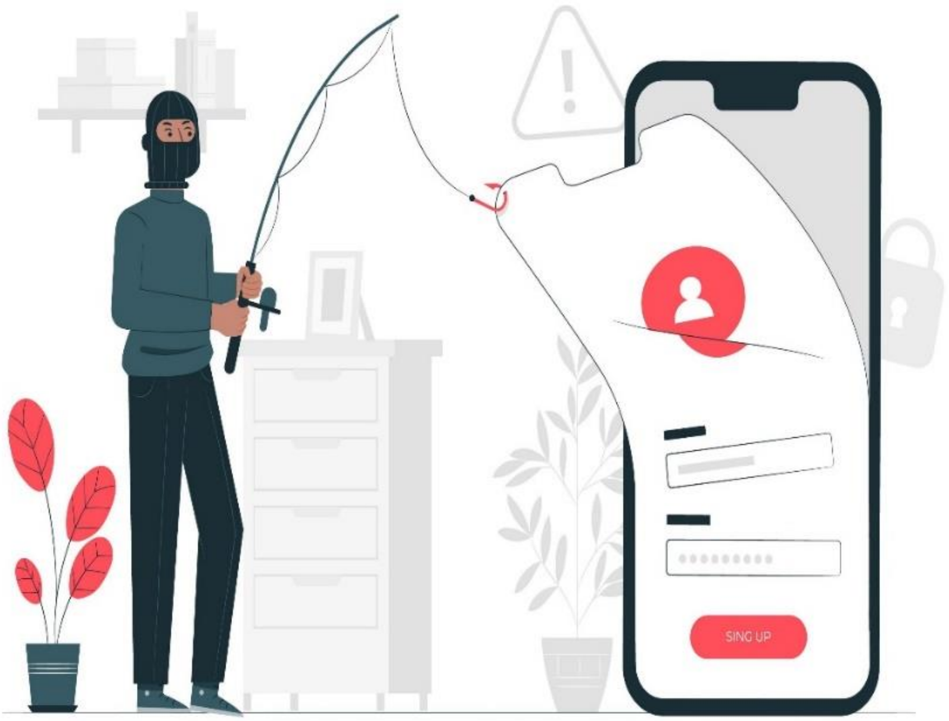


image: Freepik.com

# Reporting an email modification fraud

report@sra.**org**.uk

Warning – do not skip this bit

image: Freepik.com

# Current trends: data breaches

- Examples of sophisticated attacks: hive and M&A’s

- ICO fine: measures ‘rendered firm vulnerable’

- Prepare: people, systems and controls

# Current trends: managing ransomware risks

Solicitors Regulation Authority

- Paying ransoms creates risks
- 80% who paid ransoms were targeted again – could you face increased risks?
- Don’t be a target ... focus on prevention

# Managing regulatory risks

Solicitors Regulation Authority

- Disclose material information to clients
- Maintain their confidence
- Promptly report a serious breach

National Cyber Security Centre
a part of GCHQ

# NCSC brief to SRA Compliance Conference

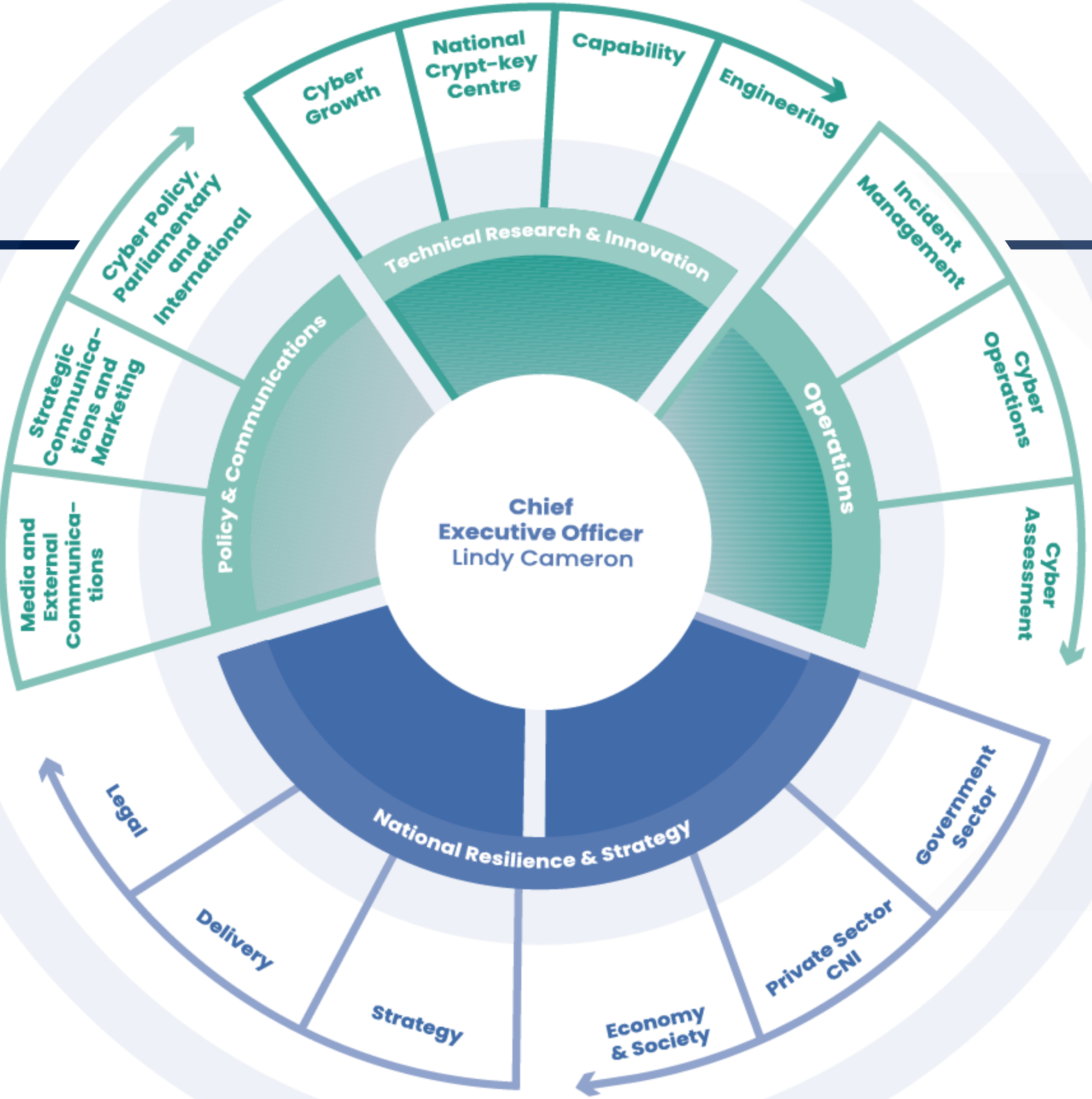
Mark K1

# National Cyber Security Centre

- The National Cyber Security Centre (NCSC), a part of GCHQ, is the UK's technical authority for cyber threats.
- Vision – Making the UK the safest place to live and work online.
- Support the most critical organisations in the UK, the wider public sector, industry, SMEs as well as the general public.
- NCSC is **not** a regulator!

National Cyber Security Centre
a part of GCHQ

# Our structure



National Cyber
Security Centre
a part of GCHQ

# Current cyber threats & trends

-Ransomware

-Supply Chain

-NCSC updates

-Cyber threat to the UK Legal sector

# Ransomware Action

Focus on infection vectors…and back up your data:

- **Remote Desktop Protocol (RDP):** RDP account compromise is the source of 50% of the ransomware attacks we see. We suggest turning off RDP or mitigate by using MFA.

- **Patch known vulnerabilities** in all remote access and external facing devices and follow vendor remediation guidance including the installation of new patches as soon as they become available.

National Cyber
Security Centre
a part of GCHQ

# Ransomware Action

- **Prevent malware spreading** across your organisation by following NCSC guidance on preventing lateral movement.
- **Back up your data effectively.** Follow NCSC guidance on mitigating ransomware attacks.

# Supply Chain Security : Understanding the problem

Threat actors target supply chain seeking easier access

More sophisticated cyber threat actors, exploit at scale

Increased outsourcing of complex IT services make it difficult to evaluate the risks

Visualisation of supply chain beyond tier one may not be possible

National Cyber
Security Centre
a part of GCHQ

# NCSC Updates

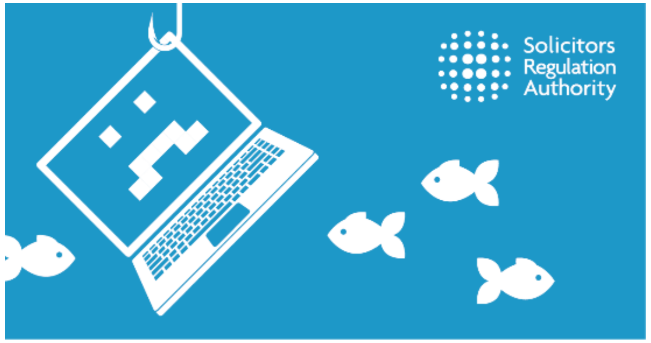
- **Cyber Essentials changes:**
  - Scoping
  - Bring your own device (BYOD)
  - Legacy software
  - Security updates
  - Statistics
- **Early warning** – new feature
- Cyber threat to UK legal sector report

# Cybercrime: panel session

Solicitors Regulation Authority

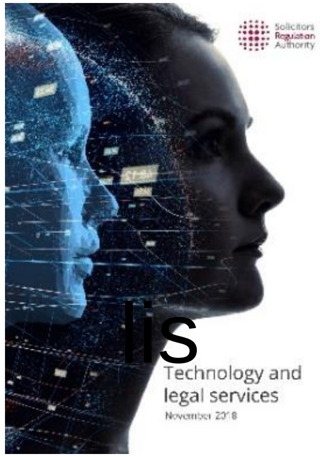
- Robert Loughlin, Executive Director, SRA (Chair)
- Rachel Clements, Regulatory Manager, SRA
- James Moss, Legal Director, Information Commission’s Office
- William Wright, Partner and Director, Paragon Insurance
- Senior representative, National Cyber Security Centre

# Help and guidance



Check our scam alerts page regularly

sra.org.uk/alerts



Cybercrime guidance and tips

sra.org.uk/cybercrime

NCSC

ncsc.gov.uk