Ransomware & data breaches

Barclays Corporate Banking

Wednesday, 20 March, 2024

BARCLAYS

Introduction

Paul Kempster, Co-Head, Mid Corporate, Corporate Banking, Barclays

BARCLAYS

Agenda

1. Introduction
2. What is a data breach?
3. Why do they happen?
4. How do they happen?
5. What to do in the event of an attack
6. The cost of an attack
7. Top 10 ransomware prevention tips
8. Resources and support

Lee Fitzgerald

Fraud Risk Strategy Director, Corporate Banking, Barclays

What is a data breach?

Any security incident in which unauthorised parties gain access to sensitive or confidential information which is then copied, transmitted, viewed, stolen, altered, used or rendered inaccessible by the attacker.

Common causes of data breaches:

Malware
e.g. ransomware delivered via phishing emails

Password compromise
e.g. through social engineering or keyboard logging

Hacking
i.e. penetration of network by exploiting IT vulnerabilities

Human error
e.g. data emailed to wrong recipient or email address

Loss or theft of paperwork

Why do they happen?

It's lucrative:

- Victims pay up - largest ransomware payout **$40m** / largest ransomware demand, over **$2bn**[1]

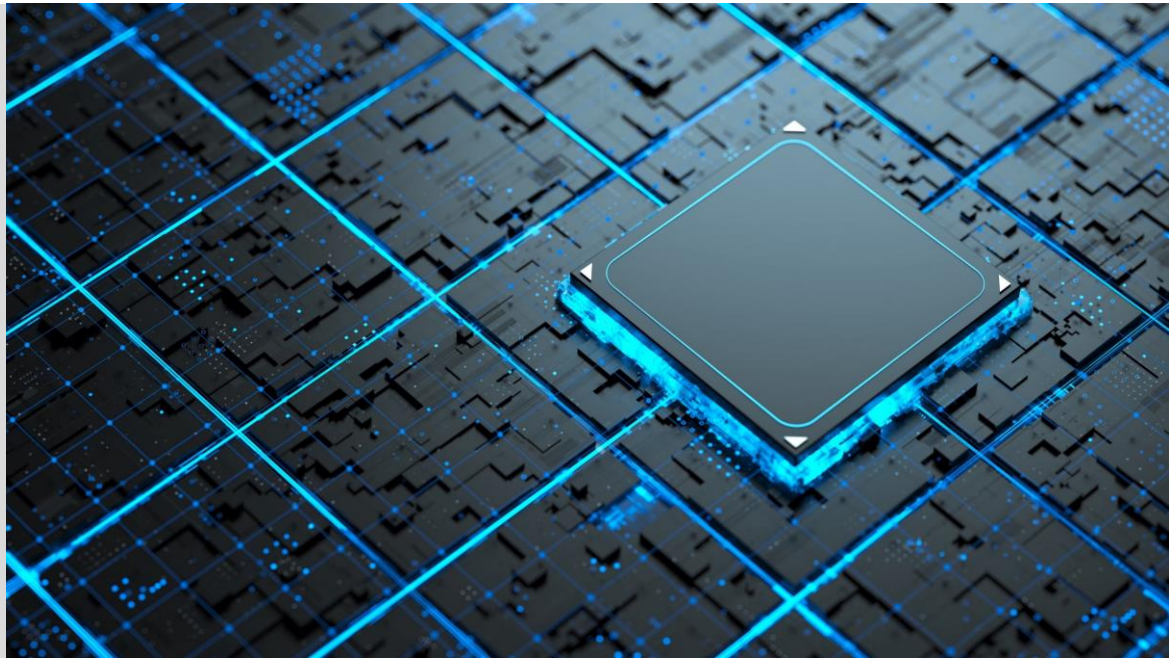
"Cybercriminals, especially those who engage in ransomware attacks had a blast in 2023. Globally, they made over $1 billion in ransoms. In one of the biggest campaigns Russia-linked Clop group exploited a vulnerability in MOVEit Transfer software and made over $100 million in ransom payments."[2]

Sources:
[1] Cyber Management Alliance
[2] Firstpost.

How do they happen? Steps 1 to 5

1	**Gaining access**	The attack is often started from social engineering techniques such as phishing or vishing. Attackers also look for open vulnerabilities to exploit.
2	**The search**	Once the attackers gain access to your network, they will start to search for the valuable data.
3	**Deployment of the ransomware**	Once the valuable data has been identified, the ransomware is triggered and starts encrypting the data.
4	**The encryption**	The attacker has now encrypted your data and possibly stolen it too (data exfiltration). Your organisation is now at a standstill.
5	**The extortion**	The extortion process begins. At this point, the ransom is demanded, usually in Bitcoin or another cryptocurrency. There are usually deadlines for making payments. If the payment is not made, there can be threats that your data will be leaked online.

What **should I do** after a ransomware attack?



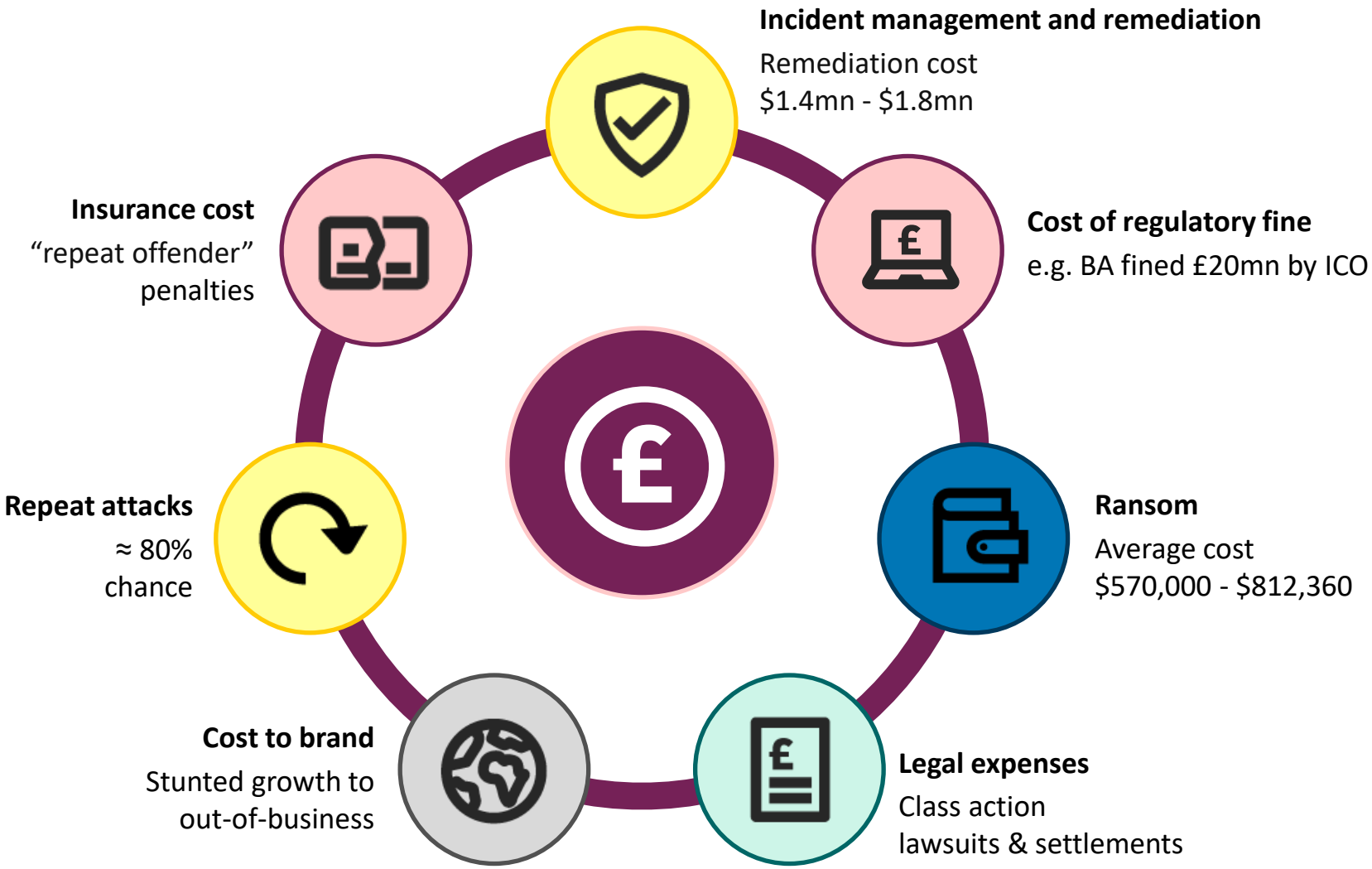
Post attack Q&As

Should I pay the ransom?	• The UK Government advises victims not to pay ransoms
How do I isolate infected systems?	• Unplug infected machines from network, mains and any storage devices • Disable network connections, including Wi-Fi, Bluetooth etc • Disable non-critical external internet connections
How do I identify the source of infection?	• This may be too technical for IT departments within your firm – if necessary, get specialist advice & resource • Contact the National Cyber Security Centre for guidance
Who do I report the attack to?	• Contact: National Cyber Security Centre (UK Gov Dept) • Regulators if applicable e.g. ICO for personal data breaches

Steve Morgan

CISO, Corporate Banking, Barclays

Estimated costs of an attack[3]



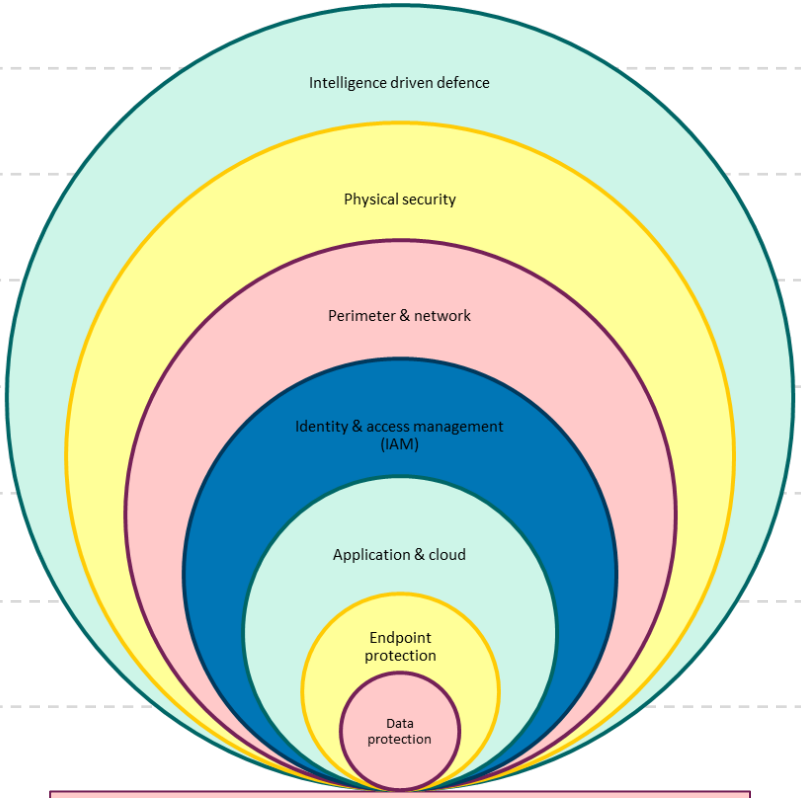
Source:
[3] diagram adapted from: cloudally

Alternatively… prevention is better than cure

Top 10 ransomware prevention tips

Note this list is not exhaustive, nor in priority order

1. Backup data
2. Keep all systems & software updated (patching)
3. Install antivirus software & firewalls
4. Network segmentation
5. Email protection
6. Application whitelisting
7. Endpoint security
8. Limit user access privileges
9. Run regular security testing
10. Security awareness training



See cyber security as a multi-layered set of defences. Barclays uses a “defence in depth” model as illustrated above. Each layer of defence needs to be in place and maintained to provide effective defence from cyber attack.

Resources and support

BARCLAYS

Ransomware checklist

Ransomware is a type of malware that disables your IT system and prevents you accessing your data, usually by encrypting files. A criminal group will then demand a ransom in exchange for decryption. The following guidance serve as an aid for your organisation to prepare in the event of a ransomware attack.

Tips to help prevent a ransomware attack

1. All devices, including mobile phones and tablets should have up-to-date antivirus or anti-malware products installed. AV updates should be loaded daily or whenever connected to the network
2. Apply strong user access controls, ideally using Multi-Factor Authentication for all privileged users e.g. IT administrators, business users with access to payments systems
3. Screen inbound email for malware, blocking and quarantining suspicious email where necessary
4. Block access to suspicious and known high-risk web-sites – security vendors have categories that can be applied by default
5. Ensure all systems are updated and patched regularly. Scan for vulnerabilities and fix them promptly
6. Ensure staff have regular training and reminders on latest malware, phishing and social engineering attack techniques and how to respond if they are targeted.

Are you prepared for a ransomware attack

1. Ensure you backup files and systems, and store them in a different location from your network or in a cloud service designed for this purpose
2. Business Continuity plans should include what to do in the event of a ransomware attack and these plans must be reviewed regularly. This should include the following as a minimum:
    - contact details for the IT department (especially if external to the organisation)
    - detail and location of critical data
    - the contact details for the National Cyber Security Centre to report the incident https://report.ncsc.gov.uk/
    - how to report the incident to your bank
    - how to bring your system back up securely
3. Test your plans and incident management processes – ensure senior stakeholders are involved and become familiar with the plan.

Barclays resources

Learn more about how to protect your business from fraud by visiting our fraud and security pages online:

Fraud Protection Hub:
https://www.barclayscorporate.com/insights/fraud-protection/

Online Fraud and Scam Toolkit:
https://www.barclayscorporate.com/insights/fraud-protection/fraud-and-scam-toolkit/

Security, Digital Channels Help Centre:
https://www.barclayscorporate.com/digitalchannels/digital-channels-help-centre/security.html

Follow us on social media:

LinkedIn - Barclays Corporate Banking

Barclays fraud support

To report fraud where payments have been sent or attempted via Barclays.net, BACS or File Gateway, call the Barclays Online Fraud Helpdesk immediately on:

0330 156 0155 (open 24/7, 365 days a year)

If calling from overseas dial **+441606566208**

To report fraud or any suspicious activity for all other products, including Business Online Banking, call Barclays UK Fraud Operations on:

0345 050 4585 (open 24/7, 365 days a year)

Calls to 03 numbers will cost the same as a call to a 01 or 02 number and will be included in any inclusive minutes. To maintain a quality service, we may monitor or record phone calls.

Report any suspicious emails purporting to be from Barclays by sending them on as an attachment to **internetsecurity@barclays.co.uk**

Additional reporting routes

- Forward text messages (Smishing) free of charge to **7726**
- Forward non-Barclays Phishing emails to the Email Reporting Service (SERS) report@phishing.gov.uk
- Fraudulent attacks, even if unsuccessful, should be reported to Action Fraud by calling:

  0300 123 2040

  Or visiting: https://www.actionfraud.police.uk/

Other resources

Take Five - Business Advice

Helping businesses to confidently challenge any requests for personal or financial information, or requests to transfer money to another account which may belong to a criminal:
https://www.takefive-stopfraud.org.uk/advice/business-advice/

Fraud Advisory Panel: Love Business. Hate Fraud.

Barclays have partnered with the Fraud Advisory Panel to help and support businesses in the fight against fraud:
https://lovebusiness-hatefraud.org.uk/

Other resources

United Kingdom

National Cyber Security Centre (NCSC):

- Mitigating Malware and Ransomware Attacks https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- The rise of Ransomware blog https://www.ncsc.gov.uk/blog-post/rise-of-ransomware
- NCSC's Early warning service https://www.ncsc.gov.uk/information/early-warning-service
- Respond & Recover https://www.ncsc.gov.uk/ransomware/home#section_7

Also from NCSC is the **Cyber Essentials** scheme and certification, strongly recommended for SME businesses
https://www.ncsc.gov.uk/cyberessentials/overview

UK Central Government
New guidelines to help directors and business leaders boost their resilience against cyber threats effective from Jan 2024
https://www.gov.uk/government/news/business-leaders-urged-to-toughen-up-cyber-attack-protections

Information Commissioners Office (ICO) - relating to data protection and data breaches
https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/

Association of British Insurers (ABI)
https://www.abi.org.uk/

Other resources

Other Jurisdictions

US Govt: Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/stopransomware/ransomware-101

US National Institute for Science and Technology – cyber security framework - Barclays uses this NIST Framework as the basis of its cyber policies and standards https://www.nist.gov/cyberframework

EU Agency for cybersecurity (ENISA) https://www.enisa.europa.eu/

European Cyber Security organisation (ECS) https://ecs-org.eu/

International Standards Organisation (OSI) - Information security, cybersecurity and privacy protection https://www.iso.org/standard/27001

Q&A

Paul Kempster, Lee Fitzgerald and Steve Morgan

BARCLAYS

Closing remarks & survey

Paul Kempster

BARCLAYS

Disclaimer

Barclays Bank PLC is registered in England (Company No. 1026167) with its registered office at 1 Churchill Place, London E14 5HP. Barclays Bank PLC is authorised by the Prudential Regulation Authority, and regulated by the Financial Conduct Authority (Financial Services Register No. 122702) and the Prudential Regulation Authority. Barclays is a trading name and trade mark of Barclays PLC and its subsidiaries.

Barclays Bank Ireland PLC is regulated by the Central Bank of Ireland. Registered in Ireland. Registered Number: 396330. Registered Office: One Molesworth Street, Dublin 2, D02 RF29. A list of names and personal details of every director of the company is available for inspection to the public at the company's registered office for a nominal fee. Calls may be recorded for security and other purposes.

Every attempt has been made to ensure that the information provided is accurate. However, neither Barclays Bank PLC ("Barclays") nor any of its employees makes any representation or warranty (express or implied) in relation to the accuracy, reliability or completeness of any information or assumptions on which this document may be based and cannot be held responsible for any errors. No liability is accepted by Barclays (or any of its affiliates) for any loss (whether direct or indirect) arising from the use of the information provided.