Cyber Incident – A Walkthrough

Andrew Rogoyski – VP Cyber Services UK

K&L GATES

CGI

Experience the commitment®

Objectives

to give you a sense of what an organisation might have to go through when experiencing a cyber attack…

…and what help you may be able to get to prepare for and prevent such an event.

K&L GATES

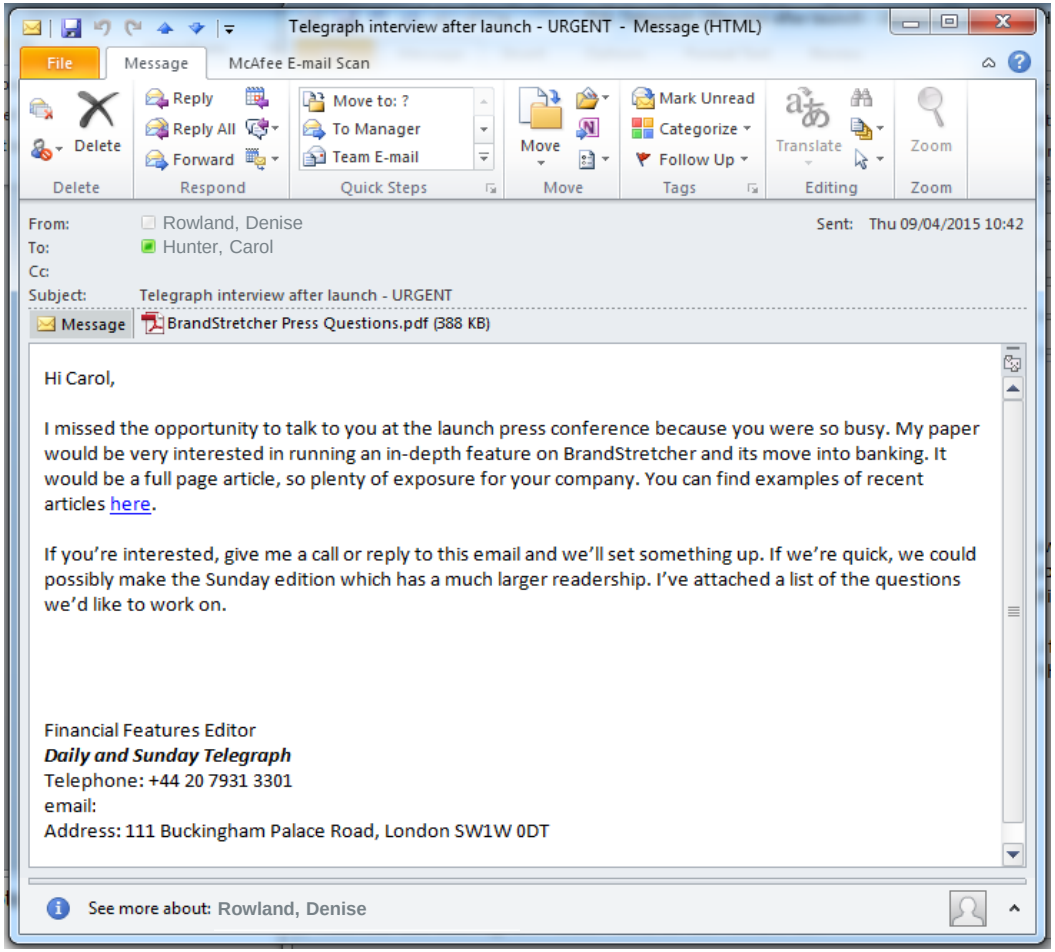
Scenario – BrandStretcher plc.

- BrandStretcher plc is a very successful **UK high street retailer** which has recently expanded into Eastern Europe and the US
- Operating in the high street and shopping malls, it has **over 10,000 staff** and an annual turnover in excess of **$2 billion**.
- BrandStretcher plc has decided to capitalise on its success in a recently launched **e-shopping portal** and customer loyalty scheme by starting its own **online retail banking services**.
- BrandStretcher plc **insource** all of their IT systems and services, running their own datacentre in Basingstoke.

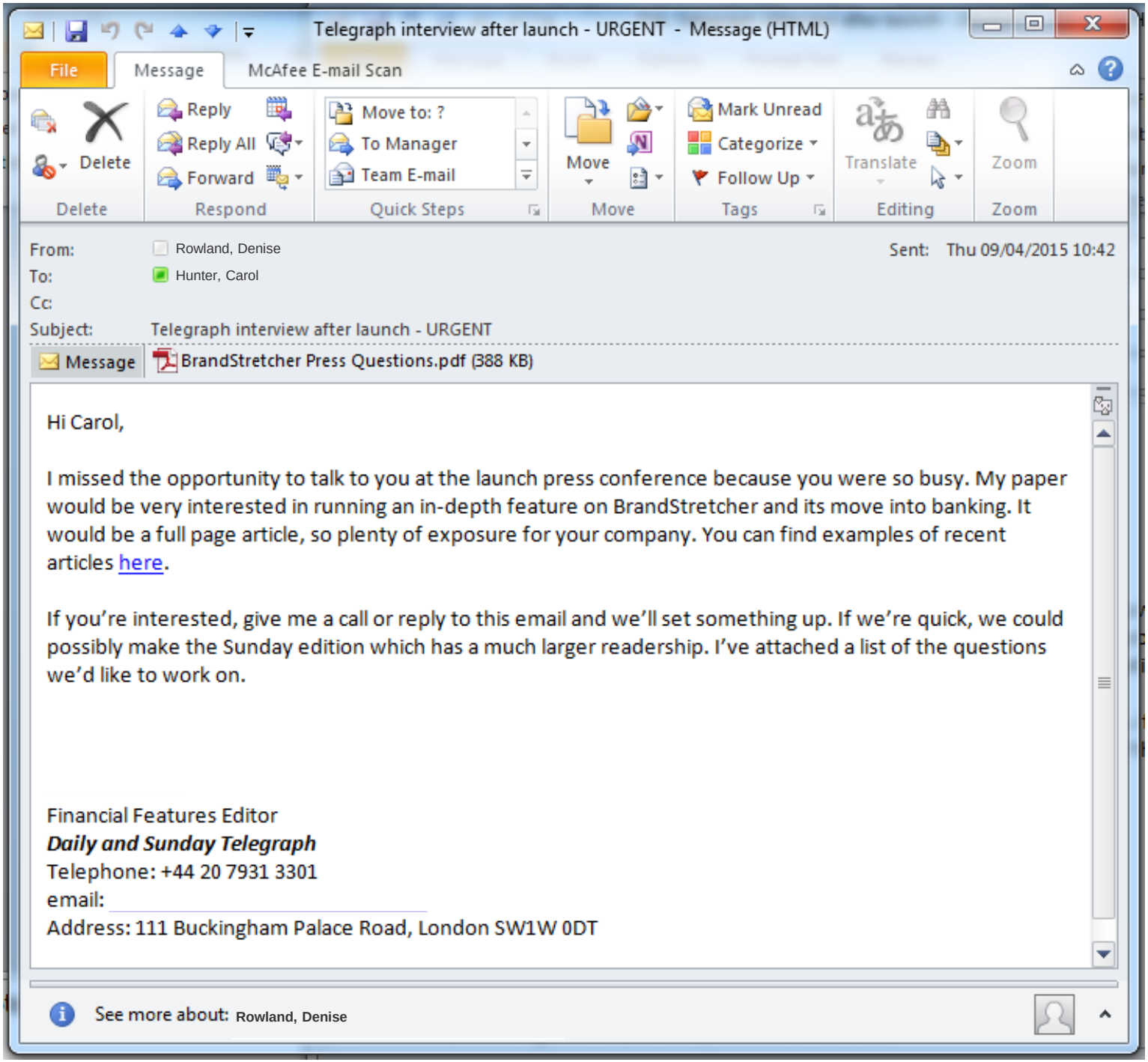
CGI

An exciting opportunity

Carol Hunter, the Head of Strategy and Marketing for BrandStretcher receives an email the day after the press announcement of the new banking project…

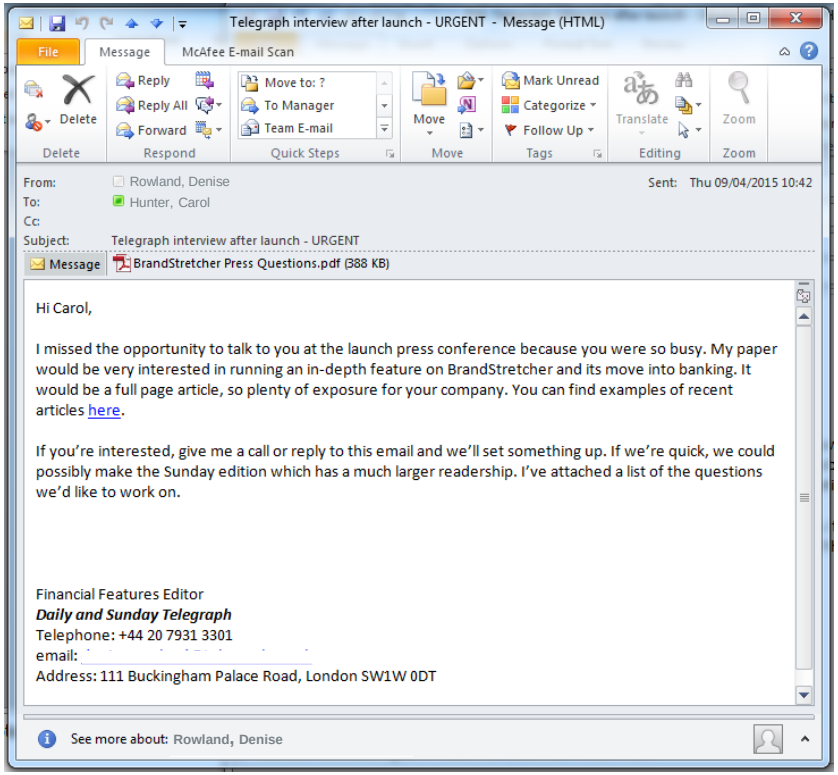


Note: The Daily and Sunday Telegraph details are used for illustrative purposes only, showing how easy it is to create a compelling and attractive phishing email based on publicly available information



Poll – Is it all right to answer this email?

1. Looks OK to me – a great opportunity
2. A bit of a surprise but I can't ignore it
3. Unsolicited, I'll ignore
4. I'll forward it to my 48 hour turnaround security team to check

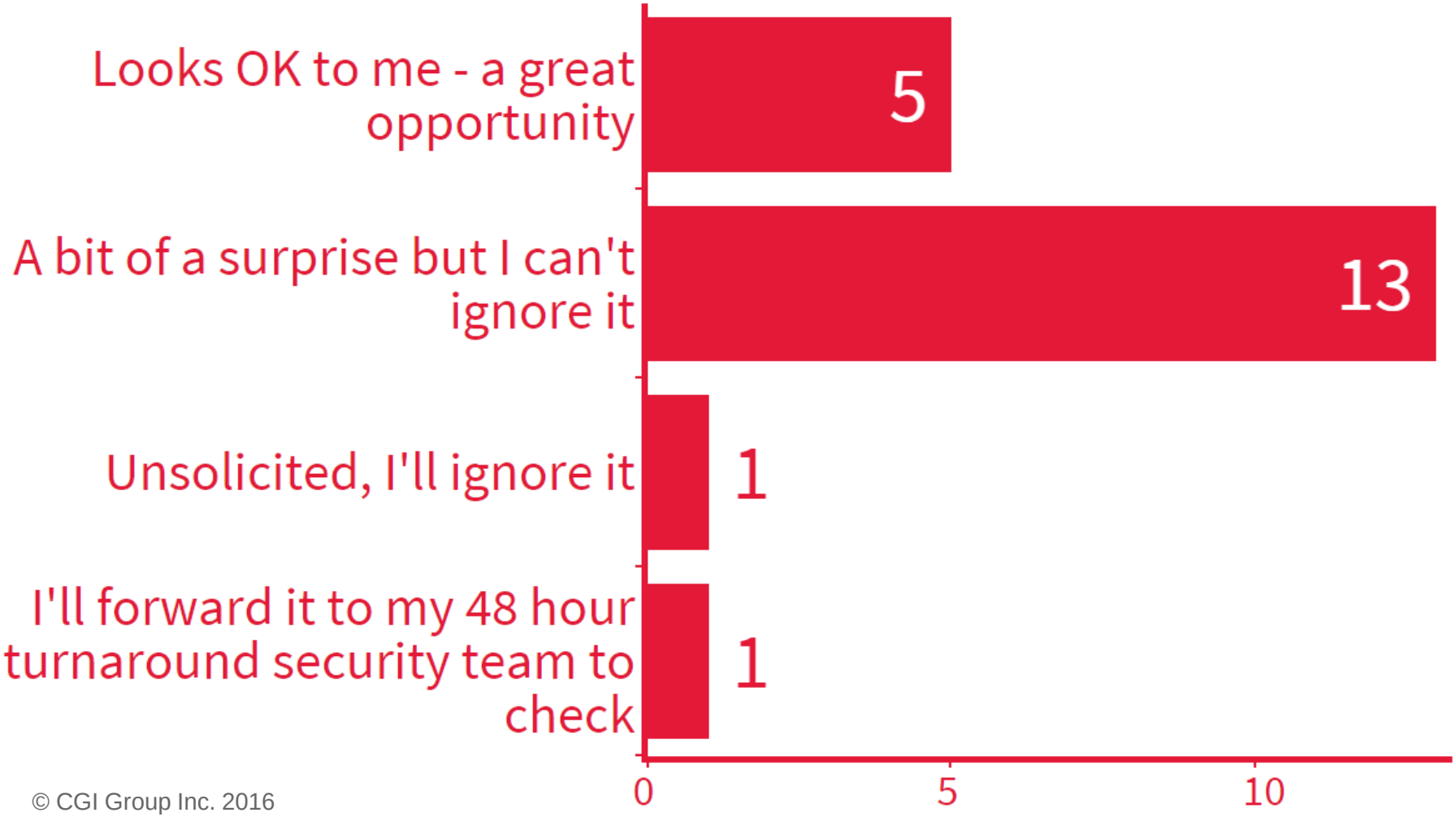


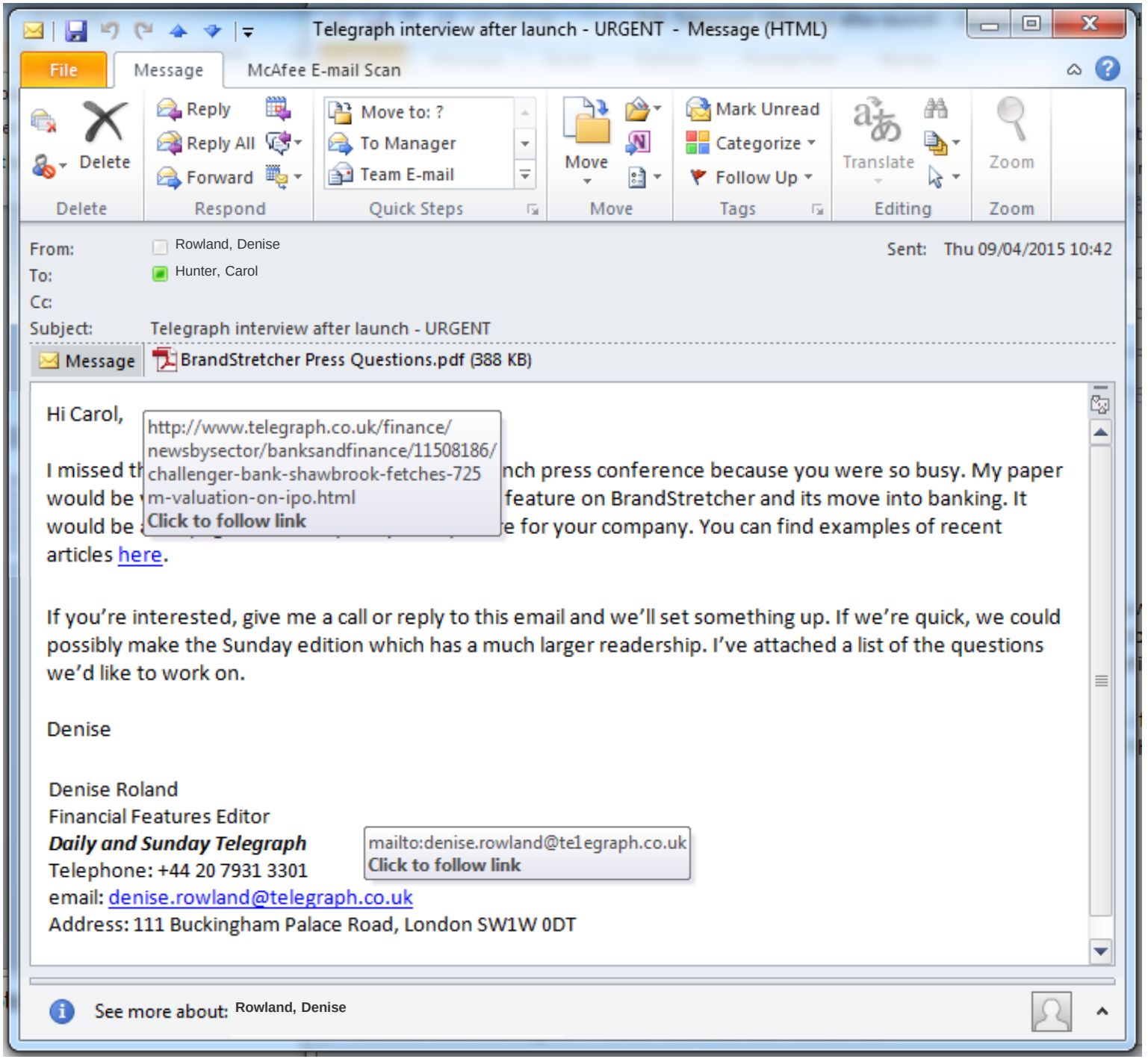
CGI
Experience the commitment®

Is it all right to answer this email?

Respond at **PollEv.com/cgicyber**

Text **CGICYBER** to **020 3322 5822** once to join, then **A, B, C, or D**





NCA Advisory

K&L GATES

- Two weeks later BrandStretcher's Director of Security receives a call from the **National Crime Agency's** Special Investigator James Blond.
- Investigator Blond advises that they have come into possession of a **complete list of BrandStretcher's staff**, including some **2,356** names, addresses, dates of employment and bank details of UK employees.
- This list was found on a **darknet forum** commonly used by identity theft gangs operating out of Eastern Europe, for sale.
- Investigator Blond advises that BrandStretcher should conduct an **immediate investigation** and recommends that they find a **cyber incident response specialist**. Blond also advises that it is unlikely that the source of the leaked data will be discovered as the forum has proven difficult to penetrate.

CGI

Poll – Reaction to the Advisory

What should BrandStretcher's priority be?

1. Reach out to the Information Commissioner's Office to advise of the incident?
2. Engage legal counsel and forensics experts to investigate?
3. Engage with law enforcement for additional help?
4. Notify the 2,356 employees of the incident.
5. Extant contractual obligations to clients on breach reporting.

CGI
Experience the commitment®

Advisory - What should BrandStretcher's priority be?

Respond at **PollEv.com/cgicyber**

Text **CGICYBER** to **020 3322 5822** once to join, then **A, B, C, D, or E**

Investigations start…

BrandStretcher engage legal counsel and a cyber security specialist.

- Legal counsel assesses the emerging scope of the breach and advises (under legal privilege) that, as the breach is serious and may lead to a risk of harm to the data subjects, the company should, as a matter of best practice, notify the ICO and other authorities.
- In addition, they should notify the FCA as the new online banking project brings them into additional regulatory interests.
- Legal counsel asks whether BrandStretcher has reviewed their contracts, security policies and recent training.
- Legal counsel asks whether BrandStretcher has cyber or other insurance that would cover some of the costs of the incident

The cyber specialists establish that BrandStretcher has never undertaken basic security testing of any of their systems, for example basic penetration testing.

- The lawyers advise that this goes against the ICO's best practise advice, so is likely to reflect badly on BrandStretcher and may lead to enforcement action being taken and aggravation of any penalties imposed.

K&L GATES

Investigations continue…

After a few hours, the cyber specialists find a number of issues including:

- A number of computers, notably clustered around the team in marketing, have had their file systems encrypted, with demands for payment being made in order to unlock the files
- Some unusual access to the senior management's shared file system with signs of large numbers of files being copied and forwarded to other parts of the company's IT infrastructure. The specialists can track the activity down to a small number of senior management users
- A number of staff are found to be using cloud-based storage and private email to transfer corporate documents to and from their home accounts
- The database on which the highly successful customer loyalty scheme resides is found to be compromised. Further investigation reveals that the scheme has recently been issuing an unusually high number of rewards

CGI

K&L GATES

Poll - Response to Investigations…

What is your priority?

1. Check the validity and scope of the company's insurance policies?

2. Disclose the loss of staff data and presence of malware to the ICO and FCA?

3. Isolate the CryptoLocker infection?

4. Confiscate the senior management's laptops and PCs for forensic analysis?

5. Suspend the customer loyalty scheme?

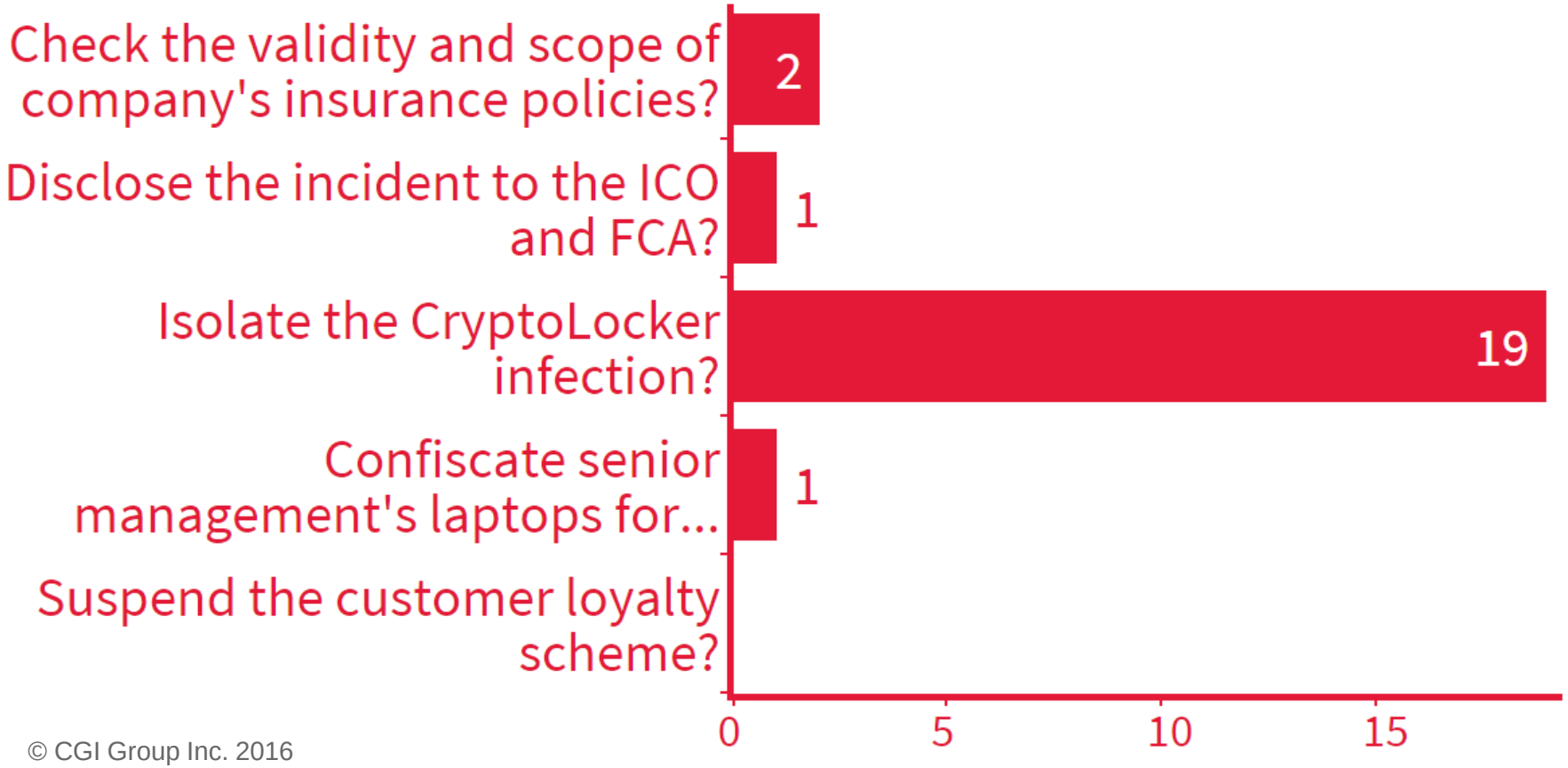
CGI

CGI
Experience the commitment®

Investigations - What should BrandStretcher's priority be?

Respond at **PollEv.com/cgicyber**

Text **CGICYBER** to **020 3322 5822** once to join, then **A, B, C, D, or E**



K&L GATES

The CEO calls for action…

The team decide to focus on eradicating the CryptoLocker infection. The CEO, now aware of the range of potential issues, demands action:

- An internal crisis management team is convened for the first time. It becomes clear that nobody is sure who is responsible for what
- The CEO insists that someone be held responsible for the situation, making it clear they would not be in their job for much longer
- The FD finds that the company's insurance policies have recently been amended to explicitly exclude claims arising from cyber security incidents
- The head of IT confirms that the marketing team haven't got a working backup system. The forensic specialists suggest the only chance they have of recovering their files is to pay the ransom

CGI

Poll – Supporting the CEO…

What is the crisis management team's priority?

1. Conduct an internal investigation on why the situation has arisen and who is to blame?

2. Pay the ransom in the hope of unlocking the marketing department's data files?

3. Roll out a training programme to raise awareness of spear-phishing attacks and how to avoid them?

4. Prepare a statement for shareholders, the staff and customers in the event of the incident becoming public?

5. Tell the 2,356 staff that their personal details have been leaked and are available for sale on a darknet forum?

CGI
Experience the commitment®

What is the crisis management team's priority?

Respond at **PollEv.com/cgicyber**

Text **CGICYBER** to **020 3322 5822** once to join, then **A, B, C, D, or E**

K&L GATES

Managing the media…

Two days later, the head of media relations receives a call from a data breach blogger and journalist:

- He wants an exclusive with BrandStretcher at the 'most senior of levels' to explore the truth of a 'massive data breach' at BrandStretcher
- He is particularly interested in knowing how this might affect their retail and new banking customers.

AND…

At the same time, the Head of HR receives an anonymous note from (presumably) a member of staff:

- They have heard staff personal information has been lost by the company
- If the company doesn't come clean with its own staff, the anonymous staffer will go to the media.

CGI

Poll – Managing the Media…

What do you do?

1. Deny all knowledge of any attack or loss of data (ignore the journalist and the staffer's threats)?

2. Make a public statement about the known loss of data and notify your own staff that they may be affected?

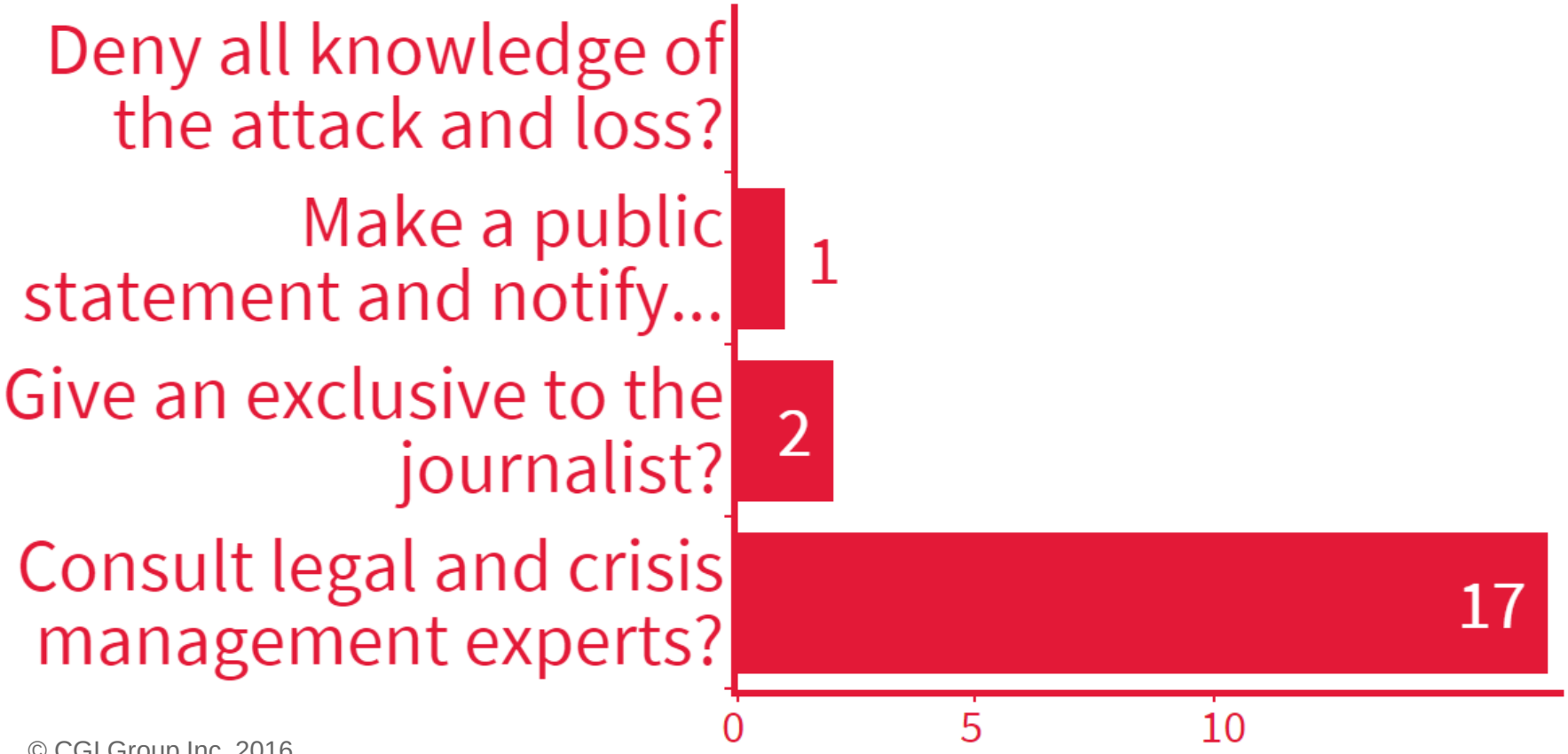
3. Give an exclusive to the journalist and insist on final editorial right?

4. Consult legal and crisis management experts?

Managing the media - what do you do?

Respond at **PollEv.com/cgicyber**

Text **CGICYBER** to **020 3322 5822** once to join, then **A, B, C, or D**



The aftermath

- The journalist publishes an article on the rumours of a breach at BrandStretcher, evidencing the story by quoting a hacker contact and an anonymous employee. The story goes viral on social media.
- The ICO and FSA opens formal inquiries on BrandStretcher's apparent failure to protect themselves adequately and to notify people potentially affected by the breach soon enough.
- A competitor uses the opportunity to take over some of the key supplier relationships, consistently outbidding BrandStretcher's deals
- The CEO fires the CIO but is publicly vilified for this act, leading to growing demand for the CEO to resign
- 10% is wiped off BrandStretcher's share price within 24 hours of the story going public
- Plans to launch the new online banking business are put on ice due to brand damage, lack of evidence of appropriate preparation and pressure from the regulator.

K&L GATES

Poll – The aftermath

Over the next year, how much did this incident cost BrandStretcher plc?

- **Less than £1million**
- **Between £1 million and £10 million**
- **Between £10 million and £20 million**
- **Over £20 million**

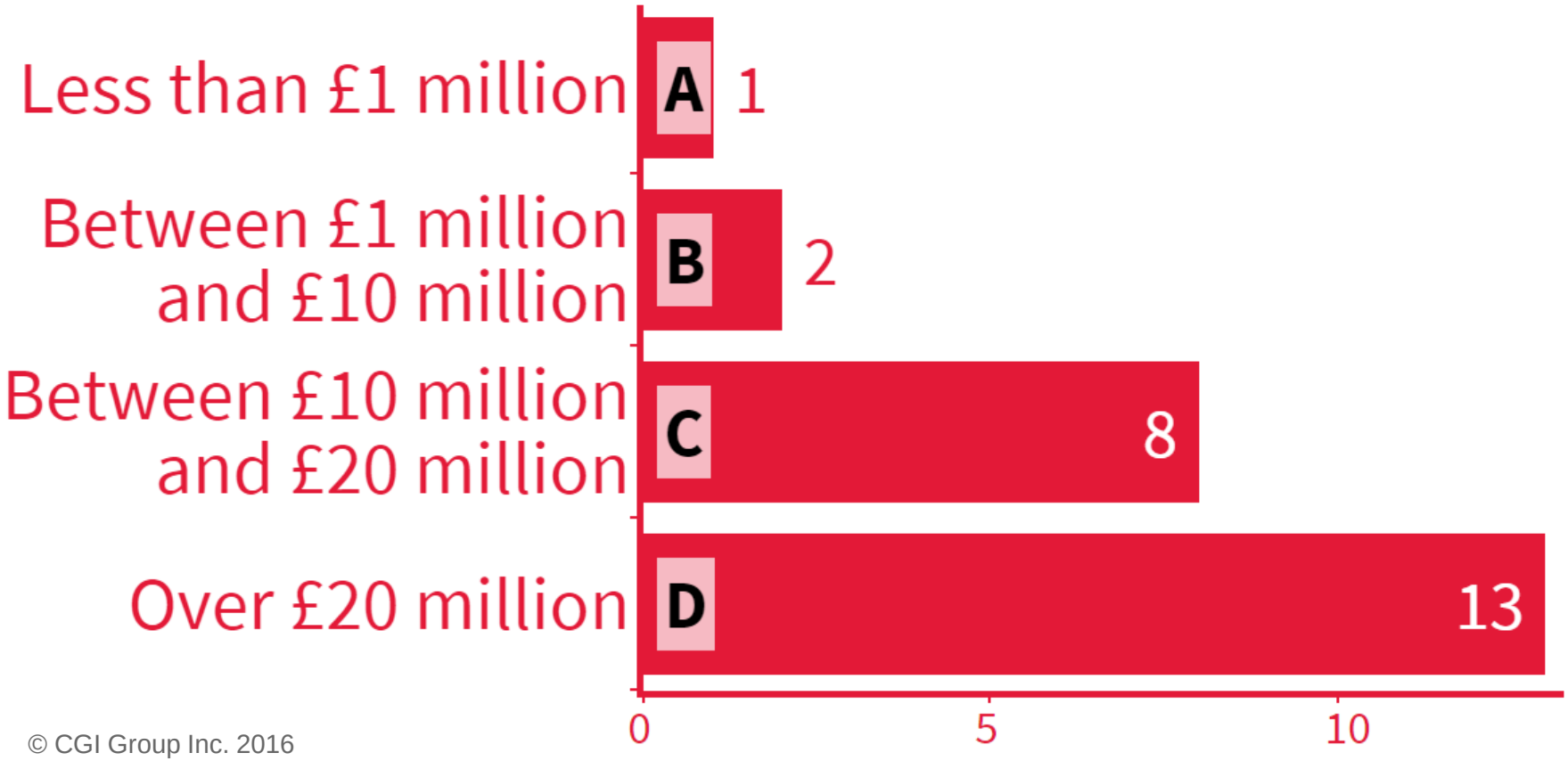
CGI

CGI
Experience the commitment®

Over a year, how much did this incident cost?

Respond at **PollEv.com/cgicyber**

Text **CGICYBER** to **020 3322 5822** once to join, then **A, B, C, or D**



Publicity and aftermath – some costs

Some of the items that could cost an organisation real money, as a consequences of a cyber attack:

- Incident management
- Breach investigation
- Technical remediation
- Data subject notification
- Call management
- Liabilities
- Direct losses
- Indirect losses
- Legal costs
- Court appearances
- Regulatory fines
- Website defacement recovery
- System & data recovery
- Extortion
- Denial of service/access
- Property damage
- Product damage
- Reputational damage
- Loss of trade secrets
- Loss of data integrity
- Loss of competitive position
- Criminal fines & penalties

Timeline – in retrospect

Timeline – in retrospect

K&L GATES

Boardroom best practice: key recommendations

Recommended eight steps to improved cyber security governance:

1. Appoint a senior executive at board level to be responsible for cyber security with the authority and know-how to address the risks. Consider any upcoming obligation to appoint a data protection officer.
2. Identify team members to make up an incident response team, including HR, legal and media communications
3. Include cyber security on every board agenda, reporting on: risk to the business, nature of sensitive data and mitigation progress at a minimum
4. Treat cyber security as a company-wide business risk and assess as you would with other key business risks, encouraging a discussion about risk appetite, risk avoidance, risk mitigation and cyber security insurance.
5. Ensure that the company understands the rapidly developing legal landscape that applies to cyber risk, including the emerging European legislation in the form of the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NISD) and the Trades Secrets Directive.
6. Get specialist expertise to advise and inform the board, whether from internal teams or external advisors
7. Set a programme of work to manage cyber risk, allowing a realistic time and budget
8. Demand improved security from your IT suppliers, including products, systems and services

CGI

Questions?

andrew.rogoyski@cgi.com
@arogoyski

http://www.cgi-group.co.uk/cyberresearch

CGI