EIGHTH ANNUAL LONDON WHITE COLLAR CRIME INSTITUTE

Cyber Crisis Management: Ready, Set? Prepare to Respond and Recover

PRESENTED BY:

King & Spalding
Panelists

MODERATOR:

Phyllis Sumner
Partner
Chief Privacy Officer
King & Spalding LLP

PRESENTERS:

Toby Duthie
Founding Partner
Forensic Risk Alliance

Meredith Griffanti
Managing Director
Strategic Communications
FTI Consulting

Dr. Jamie Saunders
Strategic Cyber Consultant
Marsh Risk Consulting

Mark Whitehead
Director
Customer Breach Support
Deloitte
Cybersecurity Landscape
Big Picture Questions

"High-impact intrusions are becoming more common; the threats are growing more complex; and the stakes are higher than ever ... That requires all of us to raise our game."

— Chris Wray, FBI Director
Cybersecurity in the Spotlight

British Airways faces $230 million fine. It would be a record under EU law.

Uber Pays $148 Million Over Yearlong Cover-Up Of Data Breach

Equifax to Pay at Least $650 Million in Largest-Ever Data Breach Settlement

Marriott Faces $123 Million Fine For 2018 Mega-Breach

Facebook lost control of our data. Now it’s paying a record $5 billion fine

Capital One hacker took data from more than 30 companies, new court docs reveal

New court documents reveal the government is investigating the Capital One hacker for 30+ other breaches.
Emerging Landscape

IC3 Complaint Statistics 2014 – 2018
The Internet Crime Complaint Center (IC3) received complaints regarding a wide array of cyber-enabled crimes affecting victims across the globe.

FINANCIAL LOSSES

<table>
<thead>
<tr>
<th>Year</th>
<th>Financial Losses</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>$800,500,000</td>
</tr>
<tr>
<td>2015</td>
<td>$1,070,700,000</td>
</tr>
<tr>
<td>2016</td>
<td>$1,450,700,000</td>
</tr>
<tr>
<td>2017</td>
<td>$1,418,700,000</td>
</tr>
<tr>
<td>2018</td>
<td>$2,706,400,000</td>
</tr>
</tbody>
</table>

TOTAL LOSSES

$7.45 BILLION

NUMBER OF COMPLAINTS

<table>
<thead>
<tr>
<th>Year</th>
<th>Number of Complaints</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014</td>
<td>269,422</td>
</tr>
<tr>
<td>2015</td>
<td>288,012</td>
</tr>
<tr>
<td>2016</td>
<td>298,728</td>
</tr>
<tr>
<td>2017</td>
<td>301,580</td>
</tr>
<tr>
<td>2018</td>
<td>1,509,679</td>
</tr>
</tbody>
</table>
GDPR – The Modern Genesis

Introduced April 2016
Proposed May 28, 2019
Effective Feb. 2019
Effective Jan. 2020
Expected 2020

2016
2017
2018
2019
2020

Amended Feb. 2017
Effective Feb. 2018
Expected late 2019
Effective Feb. 2020

EIGHTH ANNUAL LONDON WHITE COLLAR CRIME INSTITUTE
Incident Response Readiness
Incident Awareness

Companies become aware of an incident in any number of ways, including communications from:

- Third-party vendors
- Independent security researchers
- Law enforcement agencies
- Media
- Customers
- Employees
- Criminals
Incident Response

Threshold questions to answer:

• Who is responsible for assessing the incident?
• Do you collect and preserve data?
• Does this trigger your IRP?
• How do you develop a project management plan?
• Who do you involve?
• How do you develop a communications plan?
Investigating the Incident

How do you get your arms around the scope?

Do you engage a forensics firm?

Who is aware of the incident?

How do you start to develop a narrative?
Reporting the Breach

What are the legal/notification obligations?
How do you work with law enforcement?
How do you communicate to employees?
Which regulators do you notify?
What do you say to consumers and your business partners?
Do you consider a press release?
What is the risk of litigation or regulatory investigations?
The Aftermath
Legal Workflow... The Never-Ending Story
Questions?