Bristows
Data Incidents, Breach Costs and Regulatory Actions in Europe - What Lessons Have We Learned?

Robert Bond
robert.bond@bristows.com

Topics

• What have we learned post GDPR?

• Examples of internal and external threats

• How to minimise cyber risks

• Internal and external due diligence

• The cost on non-compliance
Current Cyber Incident Trends

- Payment Diversion & CEO Fraud
- Business Email Compromise
- Ransomware/Malware
- Data Breach
IBM/Ponemon Institute Cost of Breach Report 2019

- Breach lifecycle grew in 2019 by 4.9% over 2018 to 279 days
- Malicious attacks were most common and expensive
- Human error was still 49% the cause of breaches
- Companies with an incident response team and plan had a cost of breach $1.23 million less than those with an IR team and plan

Expanding Privacy Regulations

- Algeria
- Brazil
- Panama
- Cayman Islands
- Lebanon
- Bahrain
- Bhutan
- Benin
- Mauritius
- Uruguay
- Channel Islands
- South Africa
- Indonesia
- Barbados
- Kenya
- Jamaica
- Iran
- Zambia
- USA
Notifications

- Turkey – breach notification
- India – data breaches
- Japan – breaches to DPA and data subjects asap
- Brazil – ?
- Australia – breaches need to be notified if “eligible”
- USA – significant breach notification rules
- South Africa – breaches to DPA
- Russia – notification in some circumstances

USA - significant breach notification rules
Australia – breaches need to be notified if “eligible”
Often the biggest threat is ourselves

I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."

Attacks Who and Why?

<table>
<thead>
<tr>
<th>Threat Actors</th>
<th>Negligent Insider</th>
<th>Malicious Insider</th>
<th>Script Kiddies</th>
<th>Criminal Hacker</th>
<th>Nation State</th>
<th>Hacktivist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Motivations</td>
<td>easiest</td>
<td>easiest</td>
<td>easiest</td>
<td>easiest</td>
<td>easiest</td>
<td>easiest</td>
</tr>
<tr>
<td>Common Methods</td>
<td>lost device(s)</td>
<td>lost device(s)</td>
<td>lost device(s)</td>
<td>lost device(s)</td>
<td>lost device(s)</td>
<td>lost device(s)</td>
</tr>
</tbody>
</table>

- Phishing
- Exploit kits
- Ransomware
- Social engineering
- APT's
- spear phishing
- APT's
- APT's

- Phishing
- Exploit kits
- Ransomware
- APT's
- Advanced social engineering
- APT's
Internal threats
- Operator error
- Rogue employee
- BYOD
- Contractors

External threats
- Cyber criminals
- Politically motivated hackers
- Cloud, hosted solutions etc
- Cyber espionage
Computer security

• Install a firewall and virus-checking on your computers.

• Make sure that your operating system is set up to receive automatic updates.

• Protect your computer by downloading the latest patches or security updates, which should cover vulnerabilities.

• Only allow your staff access to the information they need to do their job and don’t let them share passwords.

• Encrypt any personal information held electronically that would cause damage or distress if it were lost or stolen.

• Take regular back-ups of the information on your computer system and keep them in a separate place so that if you lose your computers, you don’t lose the information.

• Securely remove all personal information before disposing of old computers (by using technology or destroying the hard disk).

• Consider installing an anti-spyware tool.

Email security

• Consider whether the content of the email should be encrypted or password protected. Your IT or security team should be able to assist you with encryption.

• When you start to type in the name of the recipient, some email software will suggest similar addresses you have used before. If you have previously emailed several people whose name or address starts the same way - eg “Dave” - the auto-complete function may bring up several “Daves”. Make sure you choose the right address before you click send.

• If you want to send an email to a recipient without revealing their address to other recipients, make sure you use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to.

• Be careful when using a group email address. Check who is in the group and make sure you really want to send your message to everyone.

• If you send a sensitive email from a secure server to an insecure recipient, security will be threatened. You may need to check that the recipient’s arrangements are secure enough before sending your message.
**Paper security**

- Manual data may still be personal data
- Keep personal data and confidential information secure
- Do not throw documents in the waste bin – shred them
- Do not leave print-outs at the printer
- Have a clean desk policy
- Have a policy on taking files out of the office
- Be aware of confidentiality in public spaces

**Staff training and security**

Train your staff:
- so they know what is expected of them;
- to be wary of people who may try to trick them into giving out personal details;
- so that they can be prosecuted if they deliberately give out personal details without permission;
- to use a strong password - these are long (at least seven characters) and have a combination of upper and lower case letters, numbers and the special keyboard characters like the asterisk or currency symbols;
- not to send offensive emails about other people, their private lives or anything else that could bring your organisation into disrepute;
- not to believe emails that appear to come from your bank that ask for your account, credit card details or your password (a bank would never ask for this information in this way);
- not to open spam – not even to unsubscribe or ask for no more mailings.
- to be wary of invitations to connect on social media
GDPR and data Breaches

Data breaches

Mandatory breach notification obligations where incident “is likely to result in a risk to the rights and freedoms of individuals”

To DPA within 72 hours

To data subjects ‘without undue delay’

Notification to DPA must describe nature of the breach including where possible the categories and approximate number of data subjects concerned and the categories and approximate number of data records concerned + contact details of DPO

Must be communicated to data subjects in clear and plain language

External due diligence

Data protection compliance

Registrations?

Breach history?

• Data Protection audit
  • Do they process personal data and sensitive data?
  • What are their data flows?
  • What are their information security policies & procedures?
  • Have they had any breaches – notified or not?
  • Who is their DPO?

• Document data processing activities
  • Consent procedures
  • Can they warrant they have rights to databases and to sell them?
  • Cookies?

• Review policies & procedures
  • Data breach response policy and procedures
  • Data sharing policy and procedures
  • Information security and cyber risk?
  • Training
Cyber Security due diligence

- How do you evaluate risk?
- Do you carry our regular assessments?
- At what level is InfoSec governed?
- Who is your CISO?
- How to do manage 3rd parties?
- Do you carry out assessments when using new technologies?
- Do you keep software fixes and support up to date?
- Do you regulate BYOD and home working?
- Do you have a cyber attack plan?
- What insurance do you have?

Internal due diligence

- Data Protection audit
  - Do you process personal data and sensitive data?
  - What are your data flows?
  - What are your information security policies & procedures?
- Document data processing activities
  - Data processing map – intra group and third parties
  - Consent procedures
  - Cookies?
- Review policies & procedures
  - Data breach response policy and procedures
  - Data sharing policy and procedures
  - DPIA and PbD and SbD
  - Training

Prepare!
- Do you need to appoint a Data Protection Officer?
- Review your T&C’s with customers/clients considering the new mandatory provisions
The EU General Data Protection Regulation

- Remedies and sanctions

- Fines of up to 4% of annual worldwide turnover may be imposed for non-compliance and without notice investigations.

- Criteria to set out the level of fine will include the degree of technical and organisational security measures and procedures implemented to:
  - Data protection by design and by default
  - Security of processing
  - Data protection impact assessment
  - Data protection compliance review
  - Designation of the Data Protection Officer

“If you think compliance is expensive – try non-compliance.”
Former U.S. Deputy Attorney General Paul McNulty

When it goes wrong!

Containment and Recovery

Evaluation & Remedy

Surviving a data breach

Assessment of Risk

Notification
Preparing for a Data Breach

• Have an incident response plan, and an incident response team, in advance
• Have a pre-selected incident response team leader
• Have outside vendors (outside counsel; fraud protection provider; forensics investigator; public relations expert) selected in advance
• Determine whether insurance coverage is adequate
• Conduct incident response drills at least annually
• Check terms and conditions of company website; do not promise more than you should
• Check employee policies and procedures
• Consider developing relationship with law enforcement authorities before the incident

Responding to a Data Breach

• Immediately notify incident response team leader
• Retain outside forensics investigator to determine extent of breach
• If appropriate, retain outside counsel
• Check insurance coverage
• Consider whether to notify law enforcement
• Determine required breach/incident notifications
• Be cautious about premature notification; don’t over-notify
• Consider when/how to notify employees
• Designate person to handle external communications
• Consider posting notice to company website
• Consider impact of any stolen intellectual property/trade secrets
• Keep ongoing record of response
Investigation Outcomes

CONTROLS
Adequate or Inadequate

ICO FINDING
Satisfactory or Negligent (Penalty)

BREACH MANAGEMENT
Swift & Efficient or Slow & Confused

RISK MANAGEMENT
Commensurate or Inappropriate

Post Breach Action
Comprehensive Controls or Inadequate

Data Breaches
That dam breach or that damn breach?
Thank you

Bristows LLP
100 Victoria Embankment
London EC4Y 0DH
T +44 20 7400 8000

robert.bond@bristows.com