DYNAMIQ

The Data is Within B*reach*

DARREN CLEARY

IT Development Manager

DYNAMIQ

What are security breaches, I hear you say…?

"… Any incident that results in unauthorised access of data, applications or computer networks, or where data has gone outside of it's intended perimeter…"

DYNAMIQ

Say what…?

External Breaches

External - Data has been intentionally viewed or stolen from outside of its authorised or intended zone.

Who cause external breaches?

- **Hackers** – Individuals or groups that break codes and passwords to gain unauthorised access to systems and data
- **State sponsored actors** – Trying to gain access to details such as email addresses and phone numbers

An Example – TalkTalk

DYNAMIQ

- First known about October 2015, potentially discovered earlier
- Partner company Carphone Warehouse also hacked in August 2015

How was the data stolen?

- Exposing flaws in the Company's website through poor design

The consequences…

- Six arrests, all under the age of 21
- Cost of £60 Million, loss of 101,000 Customers

The Register

More TalkTalking…

And for the 157,000 Customers who had their details stolen…

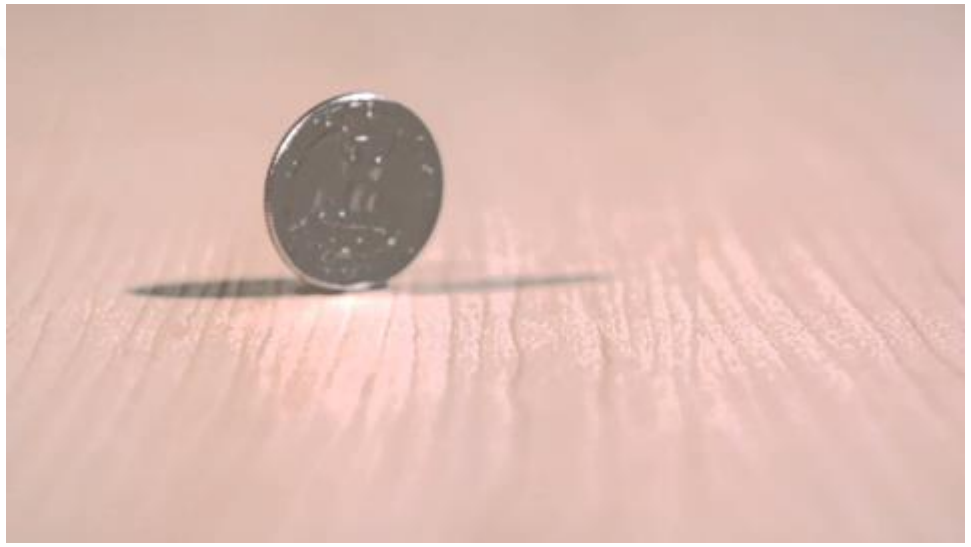
- Personal details, Bank and Credit details in the hands of unknown criminals who will use the details for gain
- Customers contacted by conmen claiming to be from TalkTalk trying to gain control of a computer to install malicious software

Flashpoint

DYNAMIQ

Most breaches we hear about on the news are external attacks from Hackers

However…



There is a flip side to breaches…

Internal Breaches

Any form of data that has been accessed without proper authorisation, either maliciously or by accident

HM Government Statistics

- **88%** of businesses had a breach within a 12 month period
  - **90%** of large organisations
  - **74%** of SMEs
- Staff related breaches
  - **75%** of large organisations, up from 58%
  - **31%** of SMEs, up from 22%
- **50%** of breaches were accidental breaches
- **50%** were malicious breaches

HM Government – 2015 Information Security Breaches Survey

Costs Of A Breach

£1.46m - £3.14m is the average cost to a large organisation

£75k - £311k is the average cost to a small business

HM Government – 2015 Information Security Breaches Survey

True costs however can not be calculated

- Company reputation
- Loss of customers
- Cost of data loss
- Business focus changes

The intangibles

DYNAMIQ

Can an SME allow for any of these to happen?

The damage has a greater effect

DYNAMIQ

Why do Malicious breaches occur?

MONEY – JOB DISSATISFACTION

- Moving to a competitor, taking client details with them
- Intellectual Property : Products or technical documents
- Financially Compromised : Blackmail
- Economic concerns

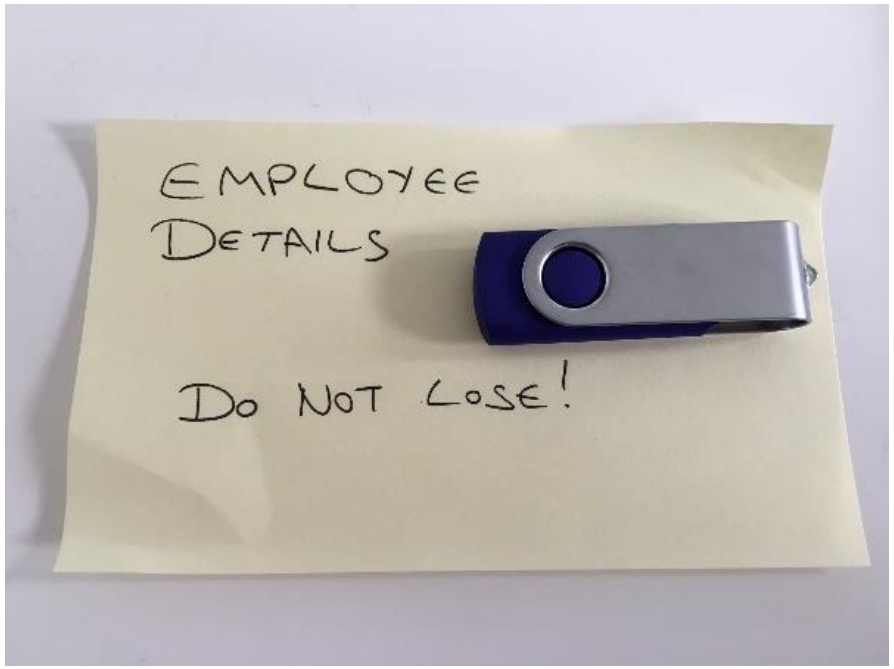
Why do Malicious breaches occur?

PRINCIPLES

- Beliefs that an Organisation is doing something wrong
- Edward Snowden – National Security Agency exposure to Phone and Internet spying
- Wiki-Leaks – Julian Assange. Exposing data of breaches publicly

DYNAMIQ

Have **YOU** ever caused an accidental breach?



Causes Of Accidental Breaches

Easiest ways to invoke an accidental breach

- Sending sensitive data to the wrong person by E-Mail
- Adapting documents that hold revision data
- Leaving data in a place outside of the Organisation
- Opening documents that contain hidden malicious software
- Introducing malware from external media
- File sharing applications to store data

An Accidental Breach

ISLINGTON COUNTY COUNCIL 2015

- Parking Charges accidently made freely available on Website
- Data included Medical information, Scanned Cheques Islington Gazette

Twice the price!

DYNAMIQ

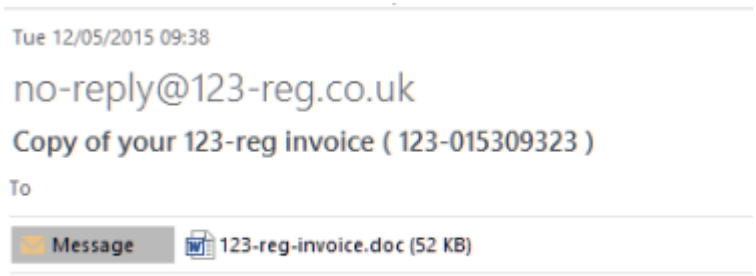
- In 2007 McLaren gained technical details of Ferrari's F1 car
  - Chief Technical Engineers exchanged documents regarding Ferrari's car and future developments
- Malicious Breach – Competitive Gain = ££££
- Accidental – Governing body leaked confidential details in PDF
  - Confidential information was blanked out. Copying text revealed details
  - Details of salaries, as well as Ferrari's technical IP. Highly secretive info exposed

HOW can we reduce the risk of a breach?

Education for Everyone

DYNAMIQ

- Implement password policies
  - Regularly change passwords, ensure complexity, advise on what to and not to use
- Help employees to recognise malicious E-mails
  - Attachments such as invoice.doc, content, or if it's a spoof sender



Manage User Privileges

- One of the major causes of Data Breach
- User Accounts
  - Enhanced privileges on Computer – Administrator / Standard User
  - Prevent installation of Applications
- Applications
  - Who has access to what Data? Employee's access data due to curiosity
  - User Accounts within Applications such as Sage products

DYNAMIQ

Application Blocking

- Prevent an application from opening
  - Removal
  - Disabling

Cloud Storage

- Ensure Security Measures
  - Use complex passwords
  - User account management
  - Location of data storage
  - Full control of data
  - Provider “Zero Knowledge”

E-Mails

- Monitoring recipients
  - Prevent Malicious breaches by blocking external mail being sent to common Public addresses such as Hotmail, Gmail and iCloud.
- Use E-Mail Content Monitoring services
  - Keyword filtering
  - Scanning of attachment types such as csv or images
- Prevent use of Employee's personal E-Mail accounts
  - Allowing access can bypass Company scanning of content
  - Block access to all E-Mail Websites such as Hotmail, Gmail and iCloud

Mobile Devices

- Smartphones have overtaken laptops as primary used devices
  - By 2017, half of the World's enterprises will have no longer supply computing devices to Employees Gartner
  - 78% of Companies say that devices connected to networks have doubled in last two years eWeek
- Mobile Malicious Software **TRIPLED** in 2015 Kaspersky Lab
- Control of devices and the Business data
  - Where is my device?
- Protection from anywhere
  - Standard for computers to have forms of protection, same applies for mobile devices
  - Use policies and tools to control mobile devices remotely, erasing data from lost devices

Curiosity Killed The Company

- USB Sticks, External Hard Drives, CDs commonly used to insecurely hold data

- People are Curious
  - If someone finds a USB device, the likelihood is that they will want to see the content. It could contain sensitive data, or malicious software

- Prevention
  - Disable Autoplay / Autorun to prevent malicious software from being run automatically if a device is plugged in

DYNAMIQ

Final Thoughts

DYNAMIQ

NO system is 100% secure from a breach, and there is no “one size fits all”

Breaches happen every day, as there is a constant shift in technology

Vulnerabilities and exploits are discovered every day, fixing can take longer

Humans will always try to find a work around whether that is from within an organisation or an outside attack

But…

DYNAMIQ

By implementing some simple steps, the risk of data breaches can be reduced. It's also important to continually review the risks

DYNAMIQ

Thank You!