Lessons Learned from the Equifax 2017 Data Breach

Graeme Payne

Former CIO Global Corporate Platforms, Equifax

Practice Leader, Strategy, Risk & Compliance, Kudelski Security

EQUIFAX

1 of 3

CRAs

Founded in

1899

10k

employees

24 countries

820m

consumers

91m

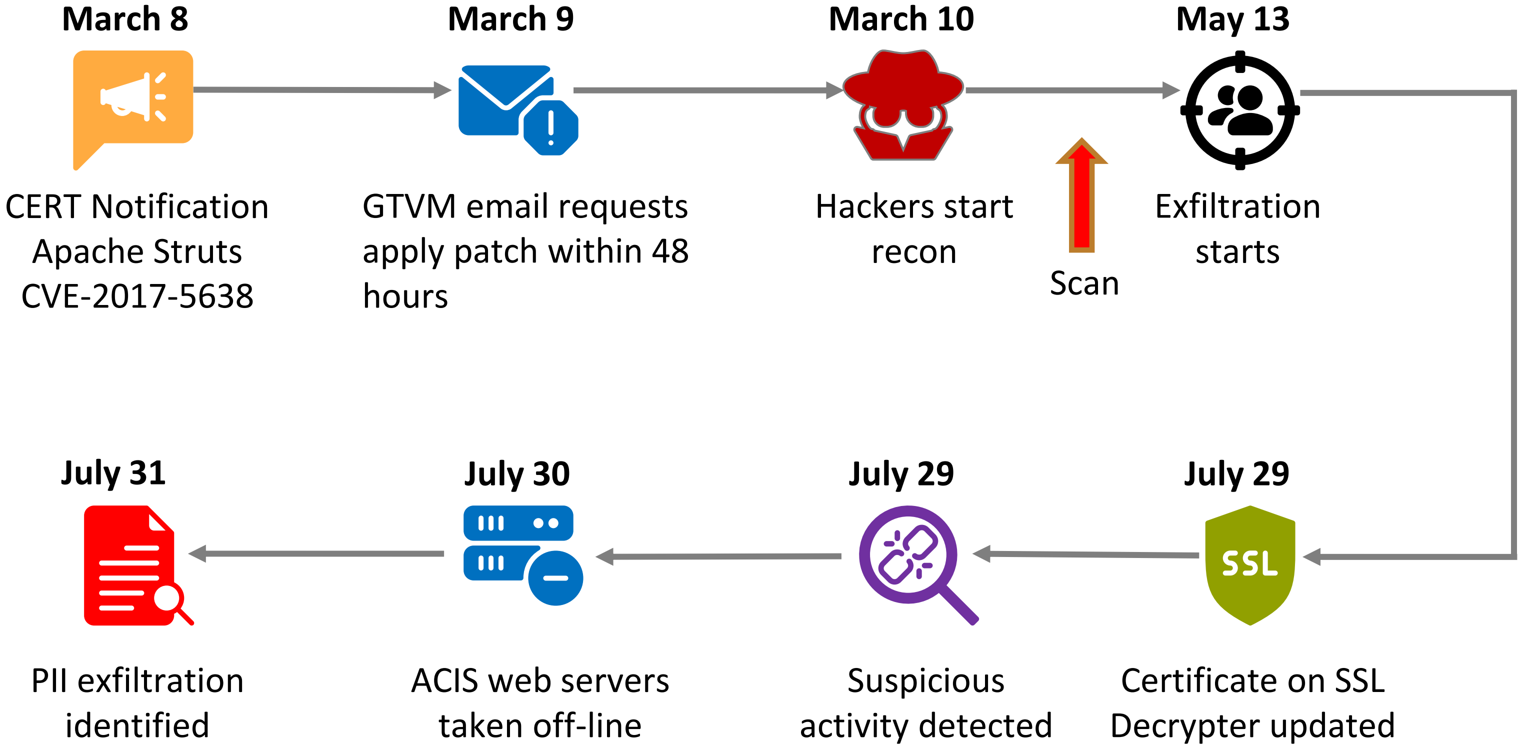
businesses

Source: US House of Representatives Committee on Oversight and Government Reform: The Equifax Breach, December 2018

PBS
Mr. Richard Smith

So the cause of the breach was....

Source: US House of Representatives Committee on Oversight and Government Reform: The Equifax Breach, December 2018



March 8

CERT Notification
Apache Struts
CVE-2017-5638

March 9

GTVM email requests apply patch within 48 hours

March 10

Hackers start recon

Scan

May 13

Exfiltration starts

July 29

Certificate on SSL Decrypter updated

July 29

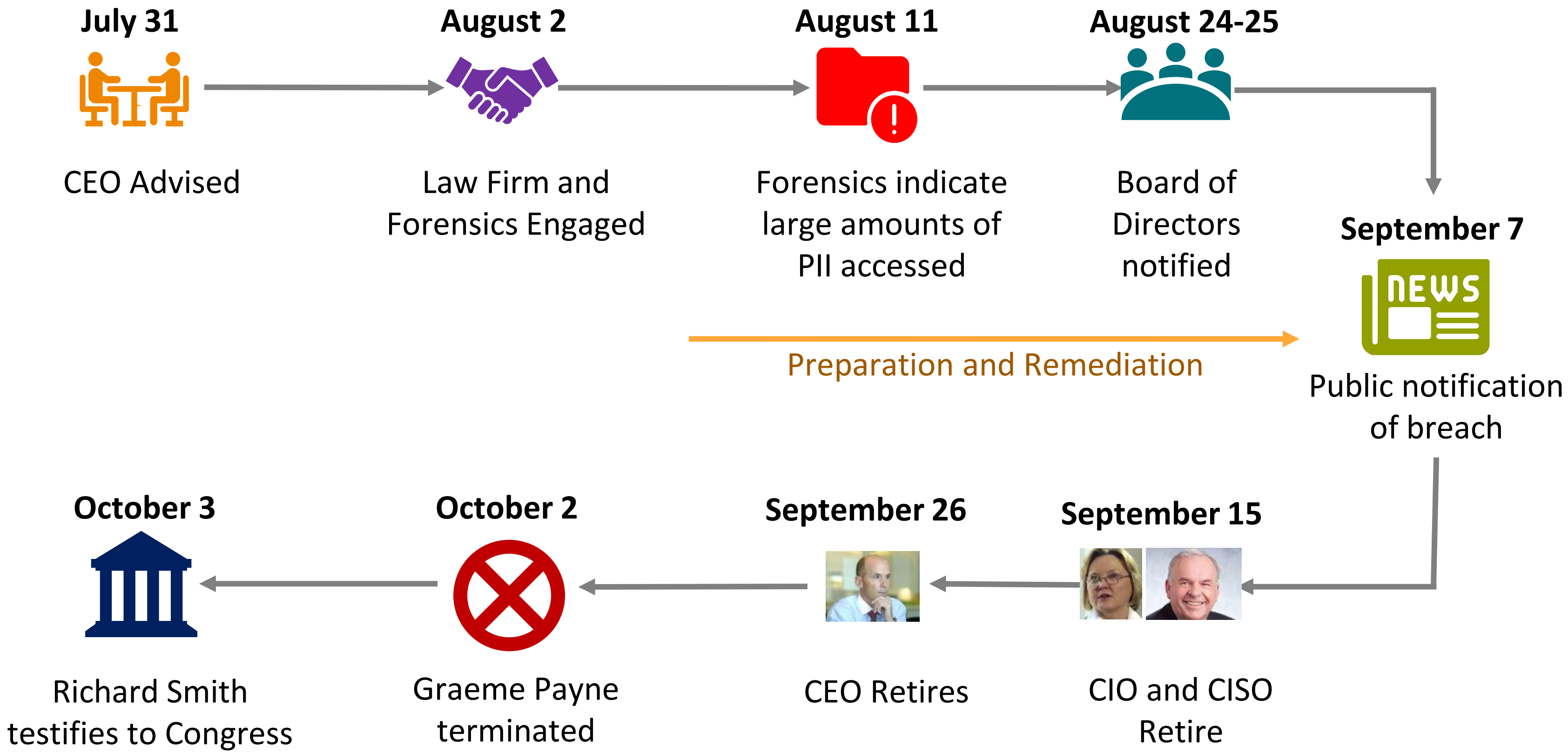
Suspicious activity detected

July 30

ACIS web servers taken off-line

July 31

PII exfiltration identified



July 31

CEO Advised

August 2

Law Firm and Forensics Engaged

August 11

Forensics indicate large amounts of PII accessed

August 24-25

Board of Directors notified

September 7

Public notification of breach

Preparation and Remediation

September 15

CIO and CISO Retire

September 26

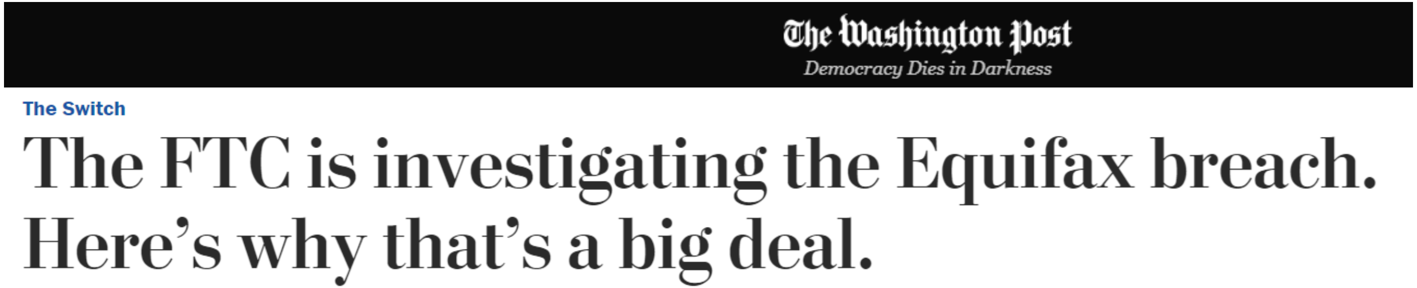
CEO Retires

October 2

Graeme Payne terminated

October 3

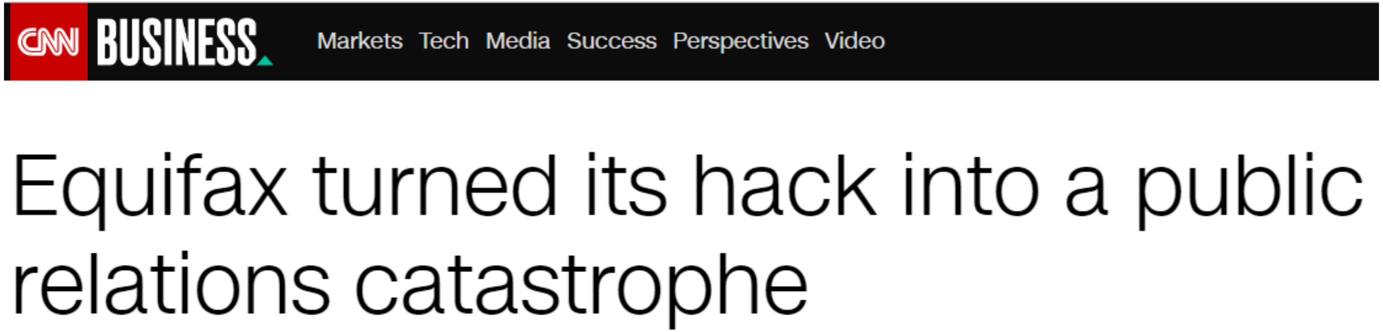
Richard Smith testifies to Congress


The Washington Post

Democracy Dies in Darkness

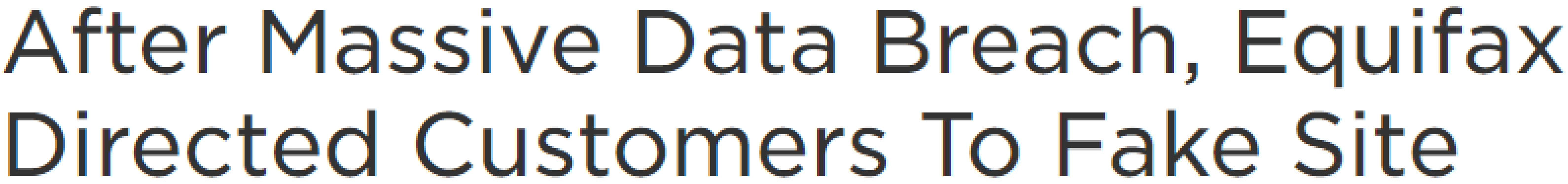
The Switch

The FTC is investigating the Equifax breach. Here's why that's a big deal.



Equifax turned its hack into a public relations catastrophe

npr


After Massive Data Breach, Equifax Directed Customers To Fake Site

EQUIFAX

Impacts

Fines: $700m

Costs: $2B+

Revenue impact

Productivity

Jobs

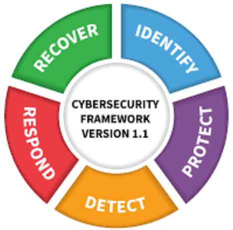
Culture

Governance

Oversight

Lessons Learned from Data Breaches

Good Cybersecurity Hygiene Remains Critical



Adopt and use security and risk framework

Establish and maintain Asset Inventory

Implement security policies

Implement protective measures

MFA

EDR

Vuln Mgmt

Patching

DLP

Monitor for Potential Issues

Configure for Logging

Utilize (or Build) a 24x7 Monitoring Service

Threat Hunting

Monitor vendors and supply chain

Be Prepared for the Inevitable

Develop IR Playbooks and IR Principles

Consider approval and procurement processes

Keep your employees informed

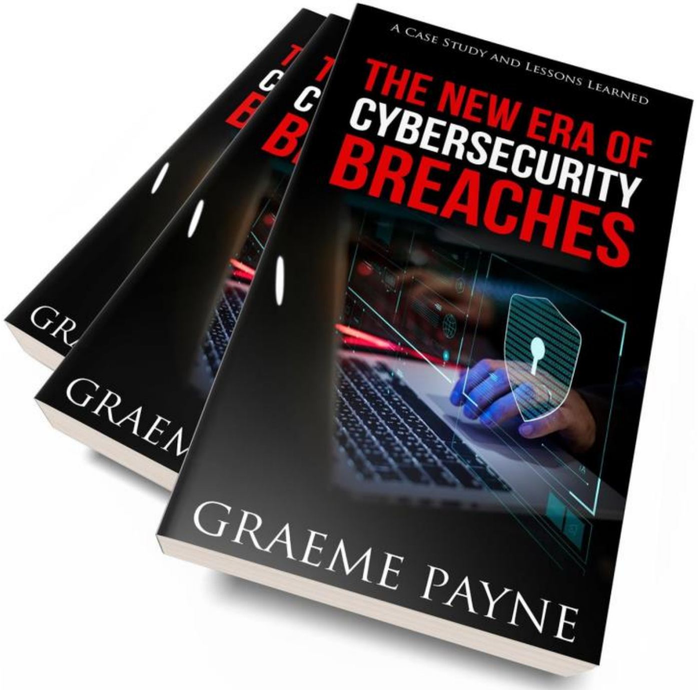
Involve senior leaders and Board

Practice media and communications management

Have IR Retainers; leverage external support

“Many times what we perceive as an error or failure is actually a gift. And eventually we find that lessons learned from that discouraging experience prove to be of great worth.”

— Richelle E. Goodrich, Smile Anyway


A Case Study and Lessons Learned
THE NEW ERA OF CYBERSECURITY BREACHES
GRAEME PAYNE

Connect with Graeme:

in ✉ graeme@cybersecurity4executives.com

About the Presenter

Practice Leader – Strategy, Risk & Compliance

Graeme Payne

CISSP, CISM, CISA
Former CIO, Cybersecurity Leader and Practitioner
Location: Atlanta

Graeme Payne has more than 30 years of IT audit. technology risk, and security experience and has worked in various industries including banking, consumer products, financial services, healthcare, and insurance. He has significant experience with information security related regulations and standards, including SOX, GLBA, HIPAA,, NIST CSF, PCI-DSS, FFIEC, SOC Audits, ISO27001. He has held leadership positions and led teams in the design and implementation information security programs for Fortune 500 companies.

As a former IT risk and compliance leader, Graeme developed and implemented information security programs to ensure the integrity, confidentiality of the organization's critical data. Graeme provided leadership and guidance across the organization, working with cross functional teams including legal, compliance and audit functions to achieve compliance to GLBA, PCI DSS, and SOX. Graeme has developed and presented business cases for investment in security and risk programs. He has regularly presented to Senior Leadership Teams and Board of Directors on risk and security.

A Case Study and Lessons Learned
The New Era of Cybersecurity Breaches
Graeme Payne

Graeme has extensive experience of managing through a major data breach, including the initial response, public notification and remediation. He has testified to congress and regulators on the breach.

Graeme holds numerous information security certifications. He is a regular speaker on cybersecurity topics. He is the author of the book “The New Era of Cybersecurity Breaches: A Case Study and Lessons Learned” and writes articles on cybersecurity topics.