



# THE HACKS THAT KEPT THEM UP MOST AT NIGHT

## OVER 2,129,000,000 RECORDS STOLEN

### THE WORST CORPORATE HACK ATTACKS IN RECENT YEARS

1 TARGET

70M RECORDS STOLEN

Thieves compromise point-of-sale terminals; make off with customer names, emails, payment card and PIN data

2 PANAMA PAPERS

11.5M RECORDS STOLEN

Email server of law firm Mossack Foneca hacked; documents leaked to media reveal money laundering schemes

3 HOLLYWOOD PRESBYTERIAN

PERSONAL RECORDS COMPROMISED

Cybercriminals seize computer systems; demand \$3.4 million ransom to release control

4 EPSILON 60M - 250M Records

Hackers gain unauthorized access to computer system and steal emails, customer names

5 YAHOO 1.5B Records

Hackers steal names, emails, phones, birth dates, hashed passwords, encrypted/unencrypted security questions and answers

6 ANTHEM 80M Records

Internal customer files breached: Names, birth dates, member IDs, SS#, emails, physical addresses, phones, employment info

7 JP MORGAN CHASE 76M Records

Periodic breaches access customer names, emails, physical addresses, phones, "internal" bank info

8 HOME DEPOT 56M Records

Hackers install malware on self-checkout payment systems

9 EXPERIAN/T-MOBILE 15M Records

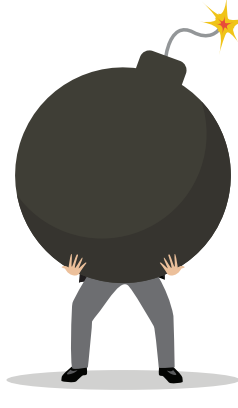
Experian network hacked; results in stolen T-Mobile customer data: Names, addresses, birth dates, SS#, driver's licenses; passports

10 PREMIERA HEALTHCARE 11M Records

Attackers access claims data: Clinical info, bank account numbers, SS#, birth dates

WEEKS, MONTHS, EVEN YEARS UNDETECTED

Experian/T-Mobile: 15 DAYS  
Yahoo: 3 YEARS



## BAD HACKS HAPPEN TO GOOD COMPANIES

Lack of attention and expertise can turn well-intentioned companies into victims

### HOW THEY GET IN

- Back doors
- SQL injection
- WiFi compromises
- Malware
- Infected point-of-sale systems
- Watering holes
- Brute force attacks
- Phishing schemes
- Unpatched versions of common web platforms (WordPress, Drupal)



### HOW COMPANIES MESS UP

- Weak credentials, a.k.a. passwords
- Disregard of security and software update alerts
- Outdated software and hardware
- Heavy reliance on WordPress plug-ins
- Server misconfigurations
- Fear of inconveniencing customers
- Security improvements and controls not a priority
- No incident response plans
- Untrained staff

### WHERE IT HURTS

Companies that fail to protect personal data suffer years of repercussions

- Business disruption
- Loss of sales revenue
- Decline in stock price
- Embarrassment and reputation damage
- Loss of shareholder, market and customer trust
- Regulatory liabilities: fines, forensics audits, monitoring fees
- Legal costs from charges by banks, credit unions, customers
- Cost of reimbursement and identity theft services

## GETTING SERIOUS ABOUT DATA SECURITY

GET THE EXPERT HELP YOU NEED TO:

- Upgrade tools, software and operating systems
- Implement best practices to replace old passwords with stronger protocols
- Put an identity and access system in place
- Guard against threats from inside and outside with the latest device authentication processes



CONCURRENCY.COM  
(866) 930-8356  
info@concurrency.com