CYBERSECURITY: TRAPS FOR THE UNWARY

DANIEL D. WHITEHOUSE, ESQ.

WHITEHOUSE & COOPER, PLLC

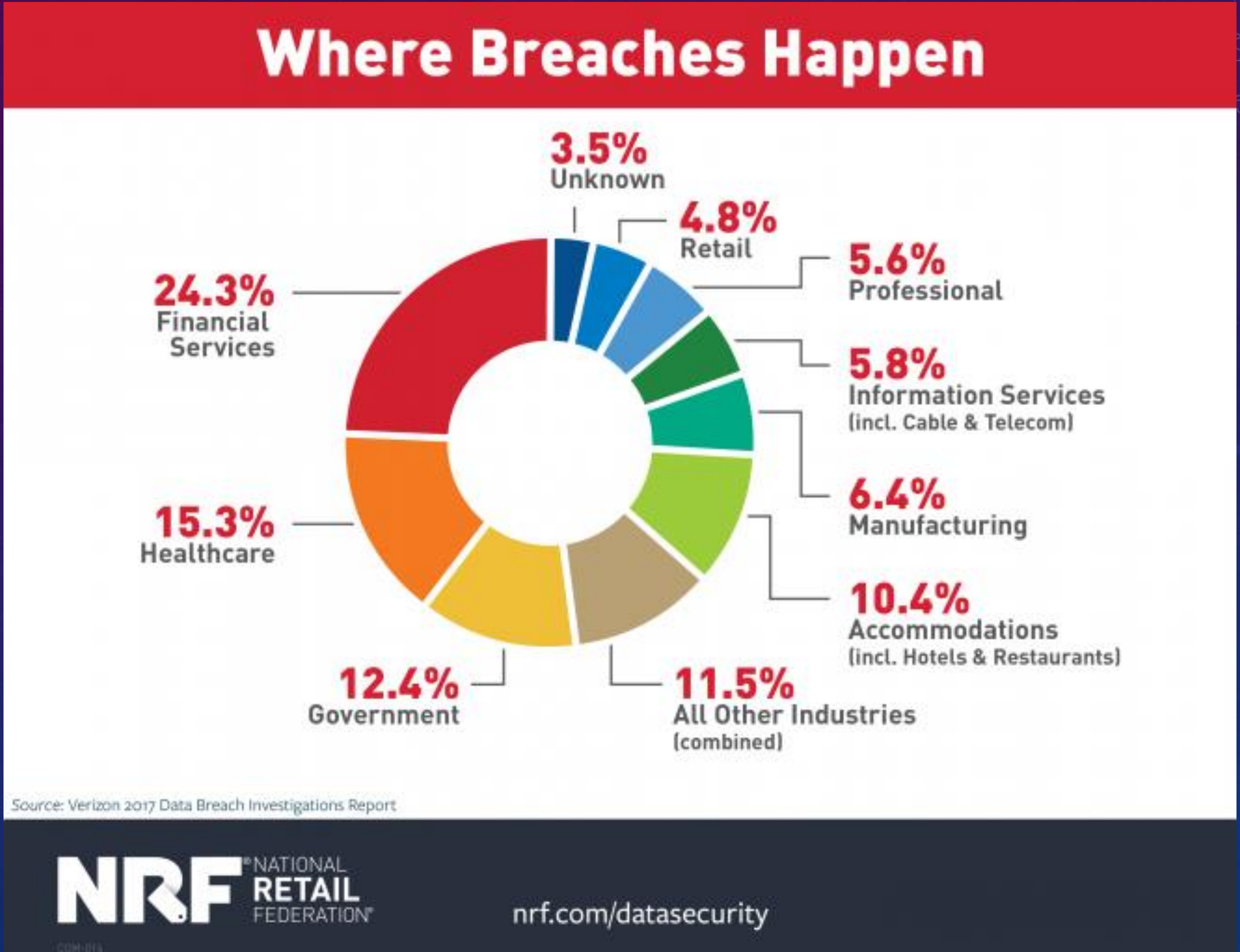
ABOUT ME

- Spent more than decade in IT
- Practice focuses on Technology and Business Law
- Degrees:
  - Juris Doctor
  - Master of Business Administration
  - Computer Science

DISCLAIMER

This session is an overview of high-level legal concepts and does not constitute legal advice. Consult an attorney to review options for your specific business needs.

DATA BREACH STATS



Where Breaches Happen

Source: Verizon 2017 Data Breach Investigations Report

NRF® NATIONAL RETAIL FEDERATION®

nrf.com/datasecurity

DATA TODAY

- Too much data!
- 96%+ of all documents are only electronic
  - Will only increase over time
- Too easy to create and save data
  - 1 GB of data = 50 Banker’s Boxes!
- Common misconceptions:
  - I’m a small business/government/department—they wouldn’t target me
  - I don’t have anything they want

MORE STATS

- Not if but when
- 72% close within 24 months
  - Down for 10 days+: 93% file bankruptcy w/in 12 months
    - 50% file immediately
- Average cost of a cyberattack is $300k

WHY SO RAMPANT?

- Growth of connected devices (including IoT)
  - ~20 billion devices connected in 2019
  - One attack makes billions of attempts
- Software can easily parse/search for personal info
- Humans still think “they” will not fall for scams
  - Behind those ~20 billion devices are humans controlling them

PERSONAL INFORMATION

- First name/initial and last name with:
    - SSN;
    - Driver’s license, ID number, passport, military ID number, etc.;
    - Financial account number (bank, credit/debit card);
    - Information regarding medical history; or
    - Health insurance policy number or subscriber ID
- User name or email address and a password

PROTECTED HEALTH INFORMATION

- Information that:
- Relates to the **past, present, or future** physical or mental **health or condition of an individual**; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and
  - **That identifies the individual**; or
  - With respect to which there is a **reasonable basis to believe** the information can be used to identify the individual.

WHERE PII LIVES

- Medical records
- Real estate files
- Employment files (Payroll services, QuickBooks)
- W9s
- ACH authorizations
- Credit card transactions (PCI compliance)
- Many, many more places

DATA BREACH LAWS

- 50 states, DC, Guam, PR, and VI have breach notification laws
- AGs have different notification requirements
- Florida: 30-day notification period
  - 500 or more requires notification to Dept. of Security
    - If more than 500,000, can notify via media
  - Fines up to $500,000
- Also consider federal notification obligations
- State laws per data type (e.g., NY notification involving SSNs)

COST OF A BREACH

- Each record * following costs:
  - Notification letter (paper, envelope, stamp: $1)
  - Credit protection ($6 - $30)
  - Help desk calls ($?)
  - Administrative fines ($??)
  - Class-action lawsuit ($???)
  - Attorneys’ fees ($????)
- Best time to engage an attorney?

DATA BREACH STEPS

- Identify the breach
- Stop the breach
    - Notify law enforcement?
- Determine what was breached
- Perform notification assessment

PCI (CREDIT CARDS)

- PCI is not law
- Set of controls relied upon by card companies
  - Current standard is 3.2.1
- Many companies can self-assess
- Standards include:
  - Build and Maintain a Secure Network
  - Protect Cardholder Data
  - Maintain a Vulnerability Management Program
  - Implement Strong Access Control Measures
  - Regularly Monitor and Test Networks
  - Maintain an Information Security Policy

PCI SAQS

- SAQ A – Card-Not-Present (ecommerce or MO/To) merchants, all cardholder data functions outsourced. Never applies to face-to-face merchants.
- SAQ B – Imprint-only merchants with no cardholder data storage. Standalone dial-up terminal merchants, no cardholder data storage.
- SAQ C – Merchants with payment application systems connected to the internet, no cardholder data storage.
- SAQ D – All other merchants (not included in descriptions for SAQs A, B, or C), and all service providers defined by a card brand as eligible to complete a SAQ.

GDPR

- Effective May 25, 2018
- Regulates “personal data”
  - Any information relating to an identified or identifiable individual
  - Includes location data, online identifiers (e.g., cookies)
- Data controllers must have consent to receive/store personal data
- Subjects must have the right to access personal data
  - And right to be forgotten
- Breach notification obligations
  - 72 hours!
  - Notify supervisory authority

OTHER FRAMEWORKS AND REGULATIONS

- NIST Security Framework
- GLBA Gramm-Leach Bliley Act of 1999 (Financial Services Modernization Act)
- Federal Fair Credit Reporting Act (FCRA)
- COPPA (Children's Online Privacy Protection Act)

COMMON THREATS

- Stolen or weak passwords used (81%)
  - Phishing scams
- Exploiting vulnerabilities
- Data loss (laptop in an Uber/airport, etc.)

PROACTIVE PROTECTION

- Antivirus/Malware protection
- Applying security updates
- Current versions of software
- User training
    - Phishing and spear phishing
    - When in doubt, don’t open it
- Layers of Security

PANAMA PAPERS

- 11.5 million documents leaked from Panamanian law firm Mossack Fonseca
- Mossack Fonseca notified clients on April 1, 2016 that its email had been hacked
- Offered a client portal with access to "corporate information anywhere and everywhere"
- Noted issues included:
  - Not updating Outlook Web Access since 2009
  - Not updating client portal since 2013
    - Drupal version noted as having at least 25 vulnerabilities

LOGICAL DEVICE PROTECTION

- Encryption
  - Hard drives (whole-disk encryption)
  - Files
  - Removable media (thumb drives)
  - Smartphones and tablets?

PHYSICAL DEVICE PROTECTION

- Smartphones
  - Password protect
  - Auto erase after X invalid attempts
  - Enable remote wipe capabilities
- LoJack®-type software for laptops
- Servers under lock and key

ERASING DATA

- Equipment Disposal
  - Use DoD erasure algorithms for devices
  - Phones as well!
  - “Brute force” method if all else fails

– Speaking of printers… they need to be erased as well!

  - And fax machines

- What about VoIP voicemails?

Don’t forget about legal holds and other requirements

PASSWORDS

- Make them complex
  - Including no children’s names…
- Change them often
- Don’t use the same ones!
  - Password tool to remember them?
- Never give them out. Ever.
  - Ever.
- Consider third-party integrations to Google, Facebook, etc.

ADDITIONAL TIPS

- Cyber Liability Insurance
- Penetration testing (including phishing)
- Data Retention Policies
  - Regulatory and Legal Hold Obligations
- Cover webcams
- Privacy shields on screens

TOMORROW’S CYBERTHREATS

- Criminals work hard; we must work harder
- Threats more complex
- Stakes significantly higher
- Cybersecurity job market explosion

QUESTIONS?

Daniel D. Whitehouse, Esq.
Whitehouse & Cooper, PLLC
201 E. Pine Street, Suite 205
Orlando, FL 32801
(321) 285-2300
Dwhitehouse@Whitehouse-Cooper.com