

ADMINISTRATIVE OFFICE OF THE COURTS



Staying Safe on the Information Superhighway

Presented By Dain Couch



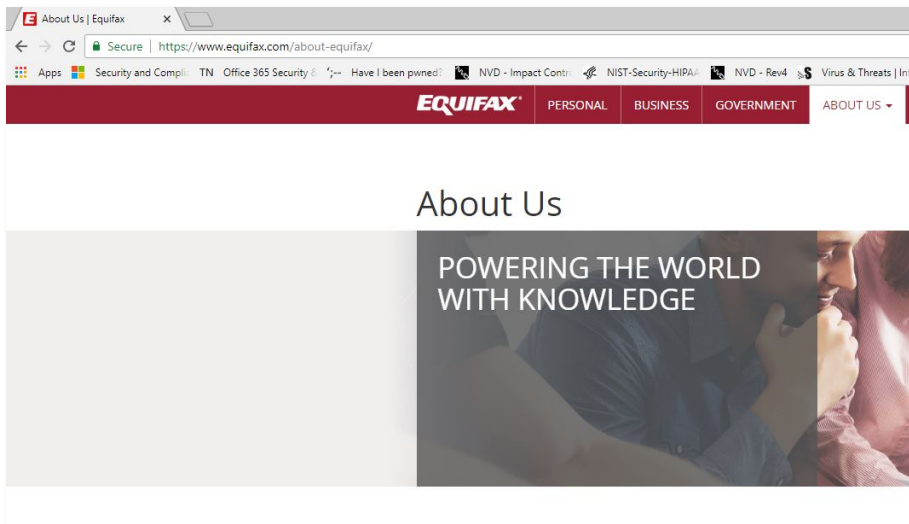
Topics

- Recent Incidents
- Court Cybersecurity Basics
- Standards



Equifax Data Breach

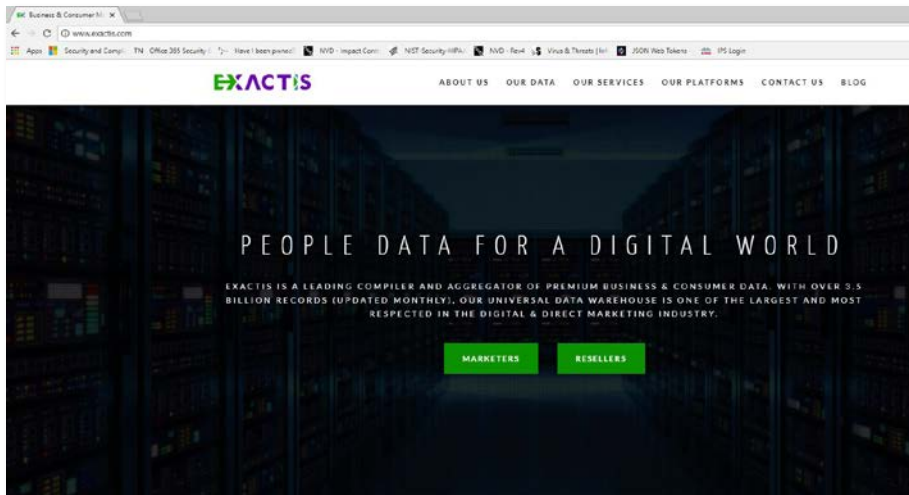
- 2017
- Your personal financial information





Exactis

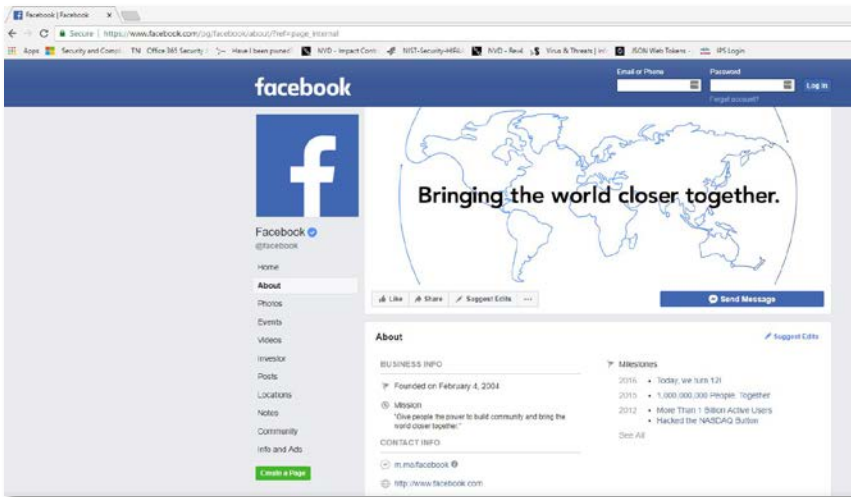
- 2018
- Your personal marketing information





Facebook

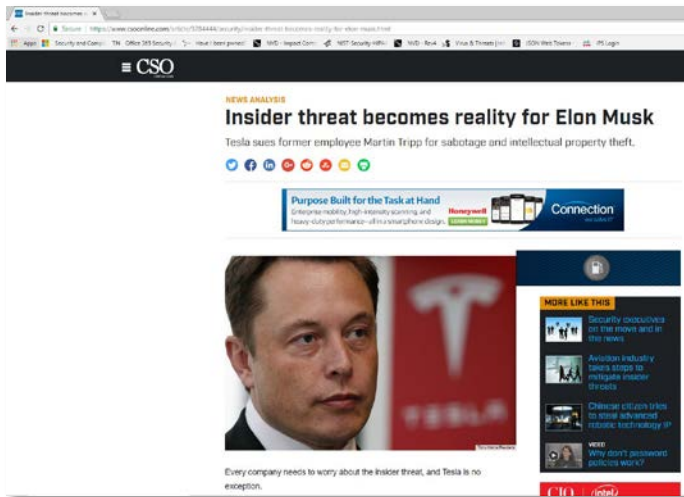
- 2018
- Your personal marketing information
- Your psyche





Tesla

- “Tesla sues former employee for sabotage and intellectual property theft.”
- Insider threat





Location Data

- Cell phone data
- Real time

A screenshot of a ZDNet article. The main headline is "US cell carriers are selling access to your real-time phone location data". Below the headline, it says "The company embroiled in a privacy row has 'direct connections' to all major US wireless carriers, including AT&T, Verizon, T-Mobile, and Sprint -- and Canadian cell networks, too". The author is "By Zack Whittaker for Zero Day | May 14, 2018 -- 10:00 GMT (12:00 PDT) | Topic: Security". There is a TechRepublic banner for a "Secure Call Platform" with a "Download Now For FREE" button. Below the banner is a screenshot of the "SECURUS Secure Call Platform" interface, showing a form for "On Demand Location Services" with fields for "Phone Number" and "Device". To the right of the screenshot is a "RELATED STORIES" section with three items: "Hardware IronKey D300 hardware-encrypted USB flash drive", "Hardware IronKey D300 Ultra durable USB flash drive with built-in encryption", and "Security Adobe fixes over 100 vulnerabilities in Acrobat, Acrobat Reader".



Ransomware

- Still going strong!
- Backups



Crypto Mining

- Alternate to ransomware
- Uses your resources

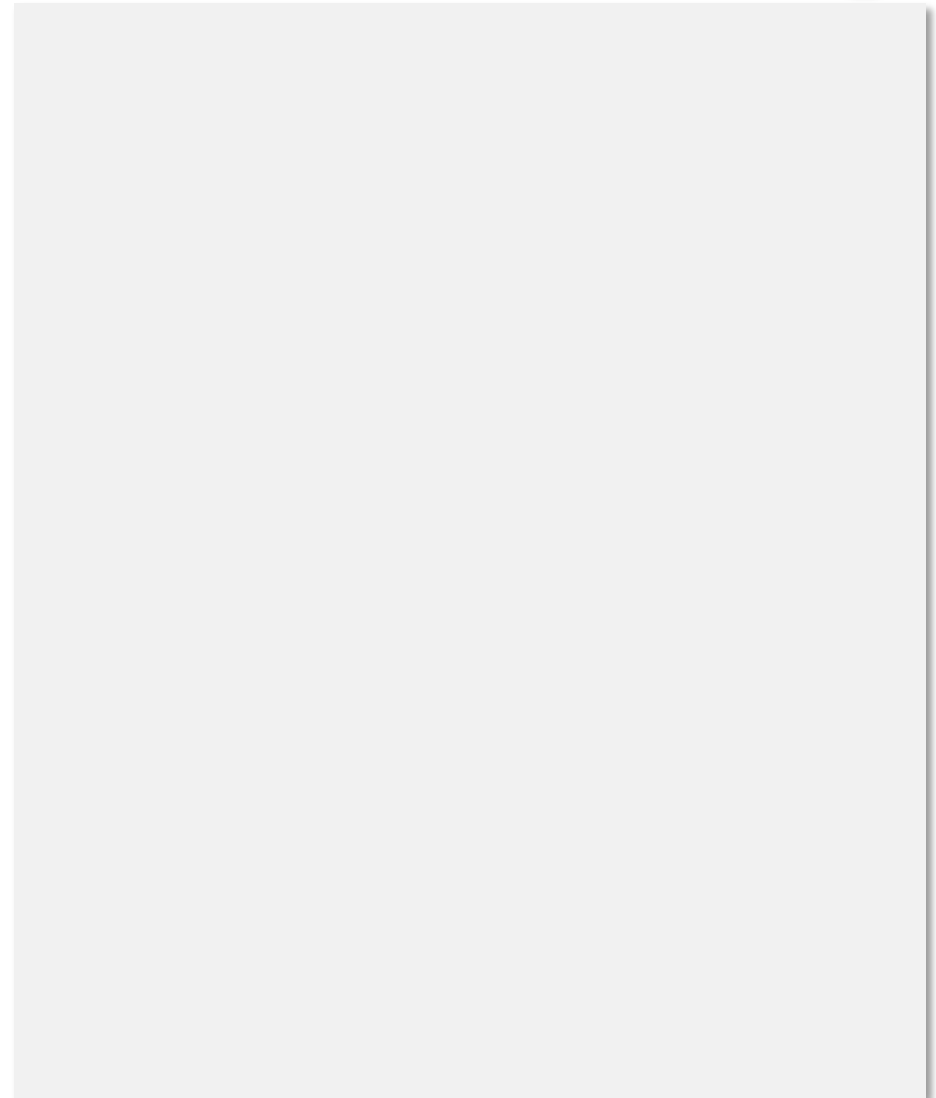




What Hackers Want

- Money
- Resources
- Information
- Fame/Status
- Just because

- White Hat - improved security/privacy





Who is Hacking

- Organized Crime
- State sponsored hackers
- Hacktivists
- Individuals – Black Hat, White Hat



FEATURE

Russia gets its super power on

BY TERI ROBINSON FEBRUARY 5, 2018

After the breakup of the Soviet Union stripped **it** of **its** influence, **Russia** seems determined to reassert itself as a **super power**...in cyberspace. Teri Robinson reports.

AOC

- Our firewall blocks 2.5 million attacks a day
- March 1, 2018 - we still received unblocked traffic from 90 countries



Layers of Defense

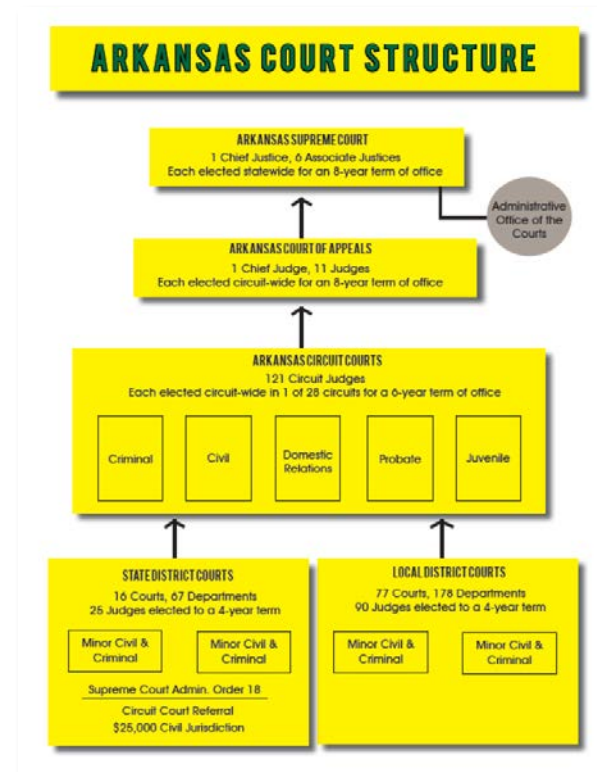
- Physical security
- IPS/IDS
- Firewalls
- Passwords
- Policy
- Antivirus
- Software updates
- Etc.





Arkansas Courts

- User Training
- Network Security
- Transmission of Data to the AOC
- Audits





Legislative Audit

- AR Legislative Audit IS Best Practices
- <http://www.arklegaudit.gov!/userfiles/editor/docs/Resources/IS%20Best%20Practices.pdf>



Top 20

- Center for Internet Security
- Controls broken down with sub-controls that align with NIST

The screenshot displays the CIS Controls website with the following content:

Basic CIS Controls

1	Inventory and Control of Hardware Assets	2	Inventory and Control of Software Assets
3	Continuous Vulnerability Management	4	Controlled Use of Administrative Privileges
5	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers	6	Maintenance, Monitoring and Analysis of Audit Logs

Foundational CIS Controls

7	Email and Web Browser Protections	8	Malware Defenses
9	Limitation and Control of Network Ports, Protocols and Services	10	Data Recovery Capabilities
11	Secure Configuration for Network Devices, such as Firewalls, Routers and Switches	12	Boundary Defense
13	Data Protection	14	Controlled Access Based on the Need to Know
15	Wireless Access Control	16	Account Monitoring and Control

Organizational CIS Controls

17	Implement a Security Awareness and Training Program	18	Application Software Security
19	Incident Response and Management	20	Penetration Tests and Red Team Exercises



NIST/OWASP



- National and International Standards
- This is what the AOC strives to implement!



Questions?