Building The Human Firewall

Andy Sawyer, CISM, C|CISO
Director of Security
Locke Lord

Cybersecurity

Cybersecurity is all about preserving the confidentiality, integrity, and availability of information assets.

- Confidentiality – Authorized parties only
- Integrity –Reliable, Authentic
- Availability – When needed to authorized parties

Cybercrime

The Internet is the crime scene of the 21st century –

NY DA Cyrus Vance, Jr.

Stealing is stealing, whether you use a computer command or a crowbar –

Carmen Ortiz, US Atty for Massachusetts

- Violent crime is down while cybercrime is up
- Tools of the trade have changed
- New Identity Theft in U.S.
  - Every 2 Seconds/1800 Per Hour

Cybercrime Drivers

- Money/Organized Crime/Nation States/Hacktivism
- Convergence
  - Internet-facing systems
  - Anything, anywhere, any time demand
  - Sophisticated attackers
- Cybercrime Consumerism
  - Hacker tools are becoming increasingly more sophisticated while requiring increasingly less knowledge by the hacker about how they work.

Cybercrime Challenges

- Attackers are hard to identify
- Crimes are:
  - Hard to detect
  - Hard to prove
  - Not reported
- Jurisdiction Issues

2014 – Year of The Retail Hack

Date	Company	Records
Jan 25	Michaels	2,600,000
Feb 6	Home Depot	20,000
Jul 22	Goodwill	868,000
Aug 18	Community Health Systems	4,500,000
Aug 21	US Postal Service	105,000
Aug 28	JP Morgan Chase	1,000,000
Nov 7	**Home Depot**	**53,000,000**
Nov 10	US Postal Service	800,000
Nov 18	Staples	1,200,000
Nov 24	Sony	500,000/100TB

2015 – Big Data Gets Its Turn

Date	Company	Records
Jan	Anthem Health Insurance	80,000,000
March	Primera Blue Cross	11,000,000
April	Office of Personnel Mgmt	21,500,000
April	RyanAir	$5,000,000
June	Trump Hotels	7 Resorts
Aug	Ashley Madison	32,000,000

Allianz Global Report:

- Cybercrime costing UK businesses £2.8bn annually
- Accounts for 16 percent of gross domestic product

Cybercrime Costs

- U.S. Firms Spent $71 Billion on Cybersecurity in 2014
- Expected to Spend $77 Billion this year
- Spending on security technology never higher
- Criminals seek to exploit networks from the inside, circumventing technology

You Probably Already Have Technology

- Firewalls
- IPS
- Email Security
- Web Security
- NIDS
- Advanced Malware Detection and Response
- Data Loss Prevention
- Endpoint AV/AS/AM
- Endpoint Encryption
- Encryption at Rest/In Motion

How To Build The Human Firewall

- Social Engineering
- Social Media
- Free
- Phishing
- Email
- Passwords
- Mobile Devices
- Wireless Networks
- Cloud Computing
- Internet of Things

Social Engineering

- The clever manipulation of the human tendency to trust.
- Malware and cybercriminals need your help.

Cybersecurity is as much social science as computer science.

- Without understanding human factors and adopting an attitude of awareness, technology will let us down.
- Technology is the cyber attack delivery vehicle.

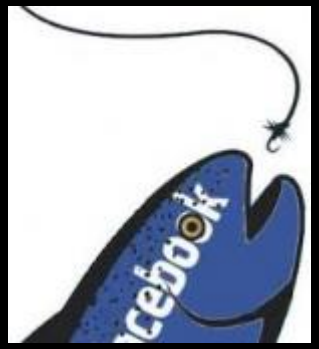
Human behavior, not computer vulnerability is the target.

Anatomy of a Social Engineering Hack

CIA Director John Brennan AOL account hacked by a teenager October 12. Brennan forwarded email from a White House email address to his AOL account.

- Hacker determined Brennan had a Verizon mobile phone.
- Called Verizon, posing as a technician unable to access the customer database. Received account number, PIN, AOL email address, and last 4 digits of credit card.
- Called AOL and asked for a password reset providing information obtained from Verizon.
- Read email, including:
  - Work spreadsheets containing names/SSNs
  - Call logs
  - Brennan's contacts

Social Media



- Don't "friend" your enemies
- Social engineering depends on familiarity
- Don't over share – 20% share full DOB
- ***Sometimes shared interests or chance meetings are more than a coincidence***
- A strong social network presence makes you 50% more likely to be spear phished
- 60% of profile pictures contain GPS data
- Messaging apps show where you've been
- Assume anything you share online will be there forever and will become public

Free

- **When the product is free, YOU are the product**

- Angry Birds
- Windows 10 EULA

  We will access, disclose, and preserve personal data, including your content (such as the content of your emails, other private communications or files in private folders), when we have a good faith belief that it is necessary to do so
- Facebook

  You grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook

Phishing

- Give a man a fish and you will feed him for a day

- Teach a man to phish and he will gladly buy dinner with your credit card

Phishing

- Phishing is the attempt to gain personally identifiable and/or financial information by masquerading as a trustworthy source in electronic communication

- **Phishing is a people problem**
  - Most popular form of Social Engineering because it works
  - Appeal to trust, relationship, charity, greed, curiosity, fear, right a wrong

Email

- 90% of malware is delivered by phishing email
  - Think Target, Chase, Home Depot, Sony
  - Think of suspicious email **You** received in the last 30 days

Making the right decision about email is your best cyber defense

Email

- Use different email accounts for work, personal correspondence, social networks
- Webmail accounts not suitable for work email
- Hyperlinks – **Hover to Discover** Before Clicking

- Recognize Fakes
  - http://chaseonline.com.zebrig.au/login.html
- Think before you reply
- Be wary of:
  - Attachments
  - Login Requests
- Resist
  - Free/Too good to be true
  - Calls To Action

Passwords

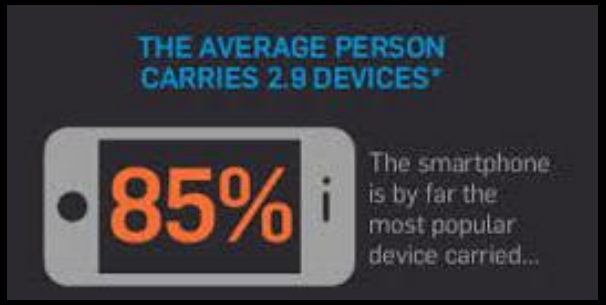
- Use Different Passwords
  - Work
  - Banking
  - Medical
  - Social Networks
  - Public Email
  - Shopping
- Change Every 90 Days/Don't Share
  - Sharing Your Password Grants Others Permission to Be YOU
  - 25 People Gave Snowden Password
- Complex passwords hard to remember
  - Epw74RG!@^
- Passphrases Instead of Passwords
  - CyberSecurity is an Attitude!
  - Cyb3rS3curity is an Attitud3!
- Password Managers

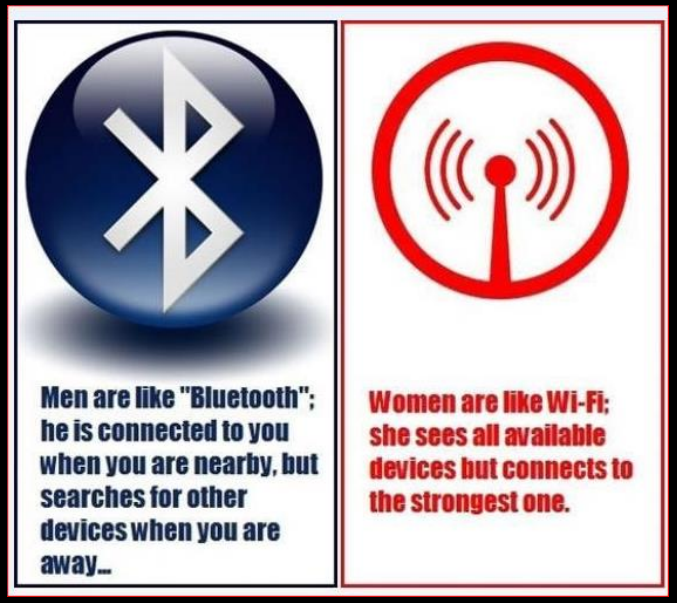
Two Factor Authentication

- Identification - Your claim
- Authentication – Your proof
  - Something you know - Password
  - Something you have - Token, text
  - Something you are – Biometrics
- You already use two factor authentication
- Use two-factor authentication for:
  - IOT
  - Websites
  - Computers
  - Remote Access

Mobile Devices

- Assume physical control equals loss
- Remote Locate/Wipe Software
- Don't be part of the jail brake
- Require Passcodes/PINs
- Encrypt everything, including memory cards
- Lock screen after 5 minutes of inactivity
- Avoid app data loss… think Angry Birds
- Turn off Frequent Locations/Bluetooth
- Dispose with care
  - 35% of resold mobile devices contain prior owner's data





Wireless Networks

- Home
  - Change the default SSID without identifying yourself.
  - Turn on encryption and select WPA or WPA/2.
  - Change the administrator name and password.
- Public
  - Encrypted or not?

  - Phones search and automatically connect
  - Hackers publish hotspots like “Free WIFI”
  - Within minutes a coffee shop hacker knows:
    - Names/Passwords/Search History/More

Cloud Computing

- Your data is in the cloud. Sanctioned or not.
  - Storage, Collaboration, Backup
  - Phone SYNC, Office Apps, CRM
- But where exactly is your data?
- And who, besides you, has access?
- **Before** moving to the cloud, ask:
  - What is/is not in Contract
  - Content Management
  - SLAs
  - Access/Subcontractors
  - Validation of controls
  - Certifications/Compliance
  - Usage of Data
  - Backups
  - Security Standards
  - Breach Notifications
  - Encryption
  - Geolocational Issues
  - Post Termination Transition Rights/Assistance
  - Support

Internet of Things

- Devices with Internet access that collect, store, and send information without human intervention
- Convenience is the priority
- Security, if at all, an afterthought
- Who has access to this information
  - Thermostats/Appliances
  - Cameras/Home Security Systems/Doors
  - Cars – GPS, Phones, Music, Directories, Insurance Devices
  - Medical devices and implants

What Should You Do?

- Recognize Social Engineering
- Minimize Social Media
- Avoid Free
- Strong/Different Passwords
- Email Discernment
- Two-Factor Authentication
- Lockdown Mobile Devices
- Encrypt Everything
- Cloud Wisely

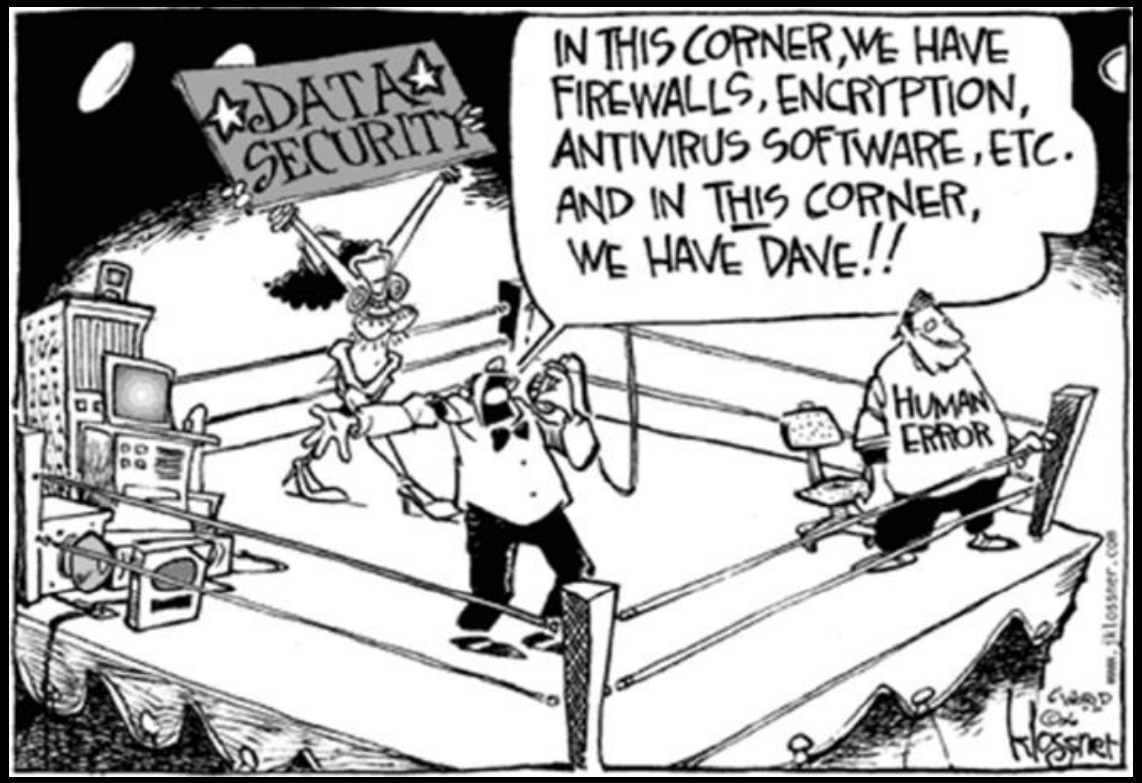
Final Thoughts

Cybersecurity is an attitude, not a department.

We spend millions on technology, and it's mostly money wasted, if we do not build the human firewall.

We strive
We persevere
We raise the bar
We get better
Be the human firewall

Questions?


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com

Helpful Links

Today's Presentation Is Available:

http://thehumanfirewall.org/presentations

http://www.securingthehuman.org