# What Every CISO Needs to Know

Presented by:
Mac McMillan
Co-Founder & CEO, CynergisTek

CYNERGISTEK

# Your Adversary Has Changed

**655,000 health records for sale on the dark web (June 28, 2016)**

**“Next time an ADVERSARY comes to you and offers you an opportunity to cover this up and make it go away for a small fee to prevent the leak, take the offer. There is a lot more to come.”**

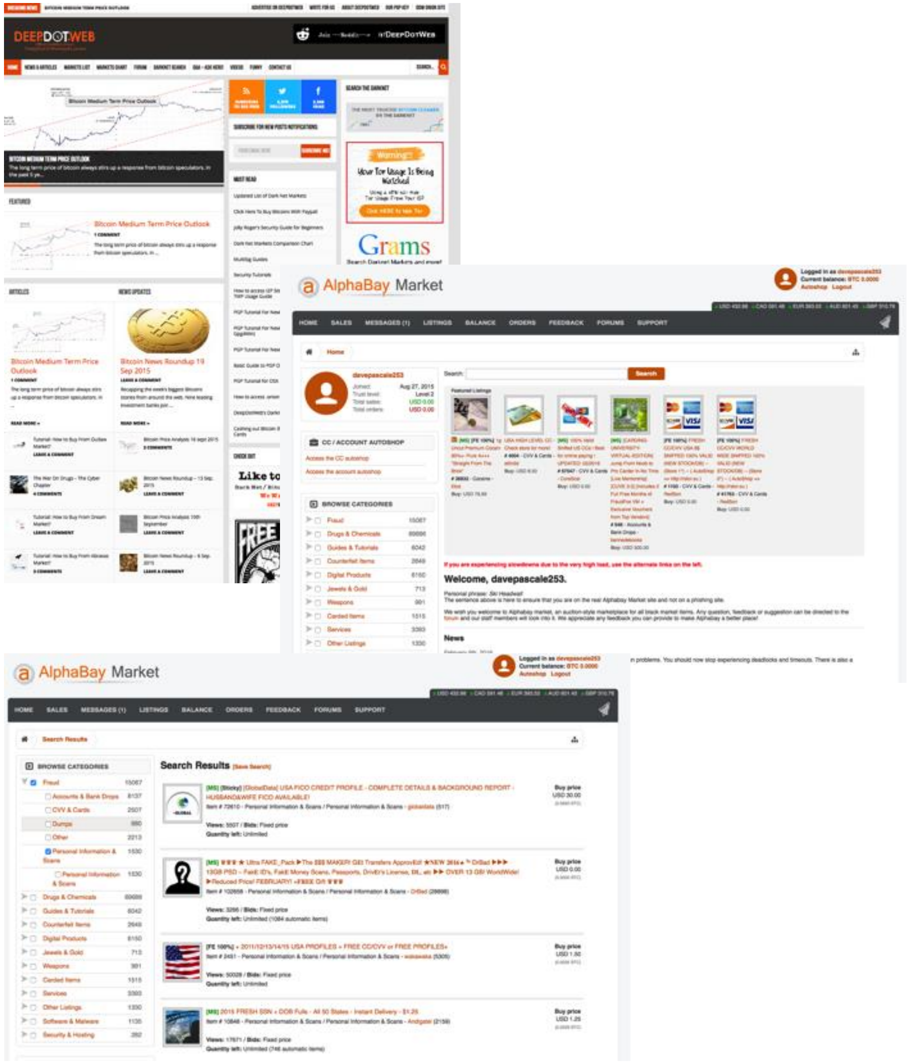
**9 million plus more health records online (June 30, 2016)**

**Healthcare HL7 Interoperability Software Source Code, Signing Keys & Licensing Database for sale (July 12, 2016)**

**“There will likely be two buyers for this, someone with nefarious intentions or someone from a small country wanting to use it for business.”**

# Opportunity is Everywhere…

- A little initiative, a curious nature, a deviant behavior, a Bitcoin wallet, PGP for encrypted communication, and a TOR browser and you are in business…
- Justice predicts $600M in revenue from cybercrime
- Its become a “for sale” industry



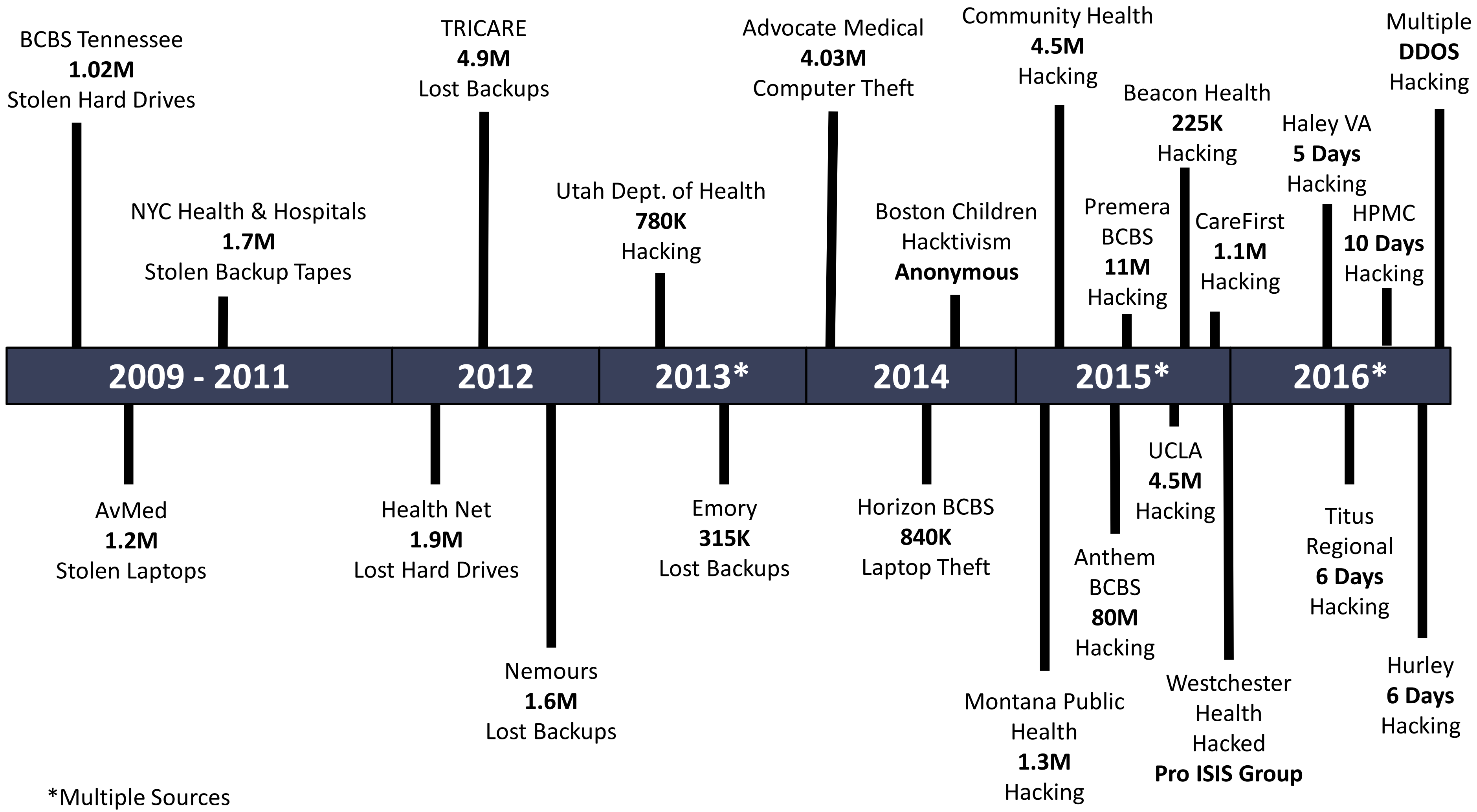
# The Stakes Are Higher

- Cyber extortion
- Cyber espionage
- Hacktivism
- Targeted attacks
- Cyber terrorism
- APTs & malware

***Motivated, Persistent & Disruptive***

# Evolving Healthcare Threat Landscape

## From lost/stolen devices to hacking



2009 - 2011

BCBS Tennessee
**1.02M**
Stolen Hard Drives

AvMed
**1.2M**
Stolen Laptops

NYC Health & Hospitals
**1.7M**
Stolen Backup Tapes

2012

Health Net
**1.9M**
Lost Hard Drives

TRICARE
**4.9M**
Lost Backups

Nemours
**1.6M**
Lost Backups

2013*

Utah Dept. of Health
**780K**
Hacking

Emory
**315K**
Lost Backups

2014

Advocate Medical
**4.03M**
Computer Theft

Horizon BCBS
**840K**
Laptop Theft

Boston Children
Hacktivism
**Anonymous**

2015*

Montana Public
Health
**1.3M**
Hacking

Community Health
**4.5M**
Hacking

Anthem
BCBS
**80M**
Hacking

Premera
BCBS
**11M**
Hacking

UCLA
**4.5M**
Hacking

Beacon Health
**225K**
Hacking

CareFirst
**1.1M**
Hacking

Westchester
Health
Hacked
**Pro ISIS Group**

2016*

Haley VA
**5 Days**
Hacking

Titus
Regional
**6 Days**
Hacking

HPMC
**10 Days**
Hacking

Hurley
**6 Days**
Hacking

Multiple
**DDOS**
Hacking

*Multiple Sources

# Ubiquitous Is The New Paradigm

- *Smart phones*
- *I0T*
- *Social media*
- *POS systems*
- *Medical devices*
- *Removable media (USBs)*
- *SPAM & email*
- *Applications*

- *Smart TVs*
- *CCTV cameras*
- *Environmental systems*
- *Downloads*
- *Attachments*
- *Browsers*
- *Wearables*
- *Telehealth*

IOT CONTROL
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore.
LEARN MORE
IOT COMFORT
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore.
LEARN MORE
IOT SECURITY
Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore.
LEARN MORE

***Threats are introduced from all directions, simple compliance strategies will not suffice, an integrated set of controls is needed.***

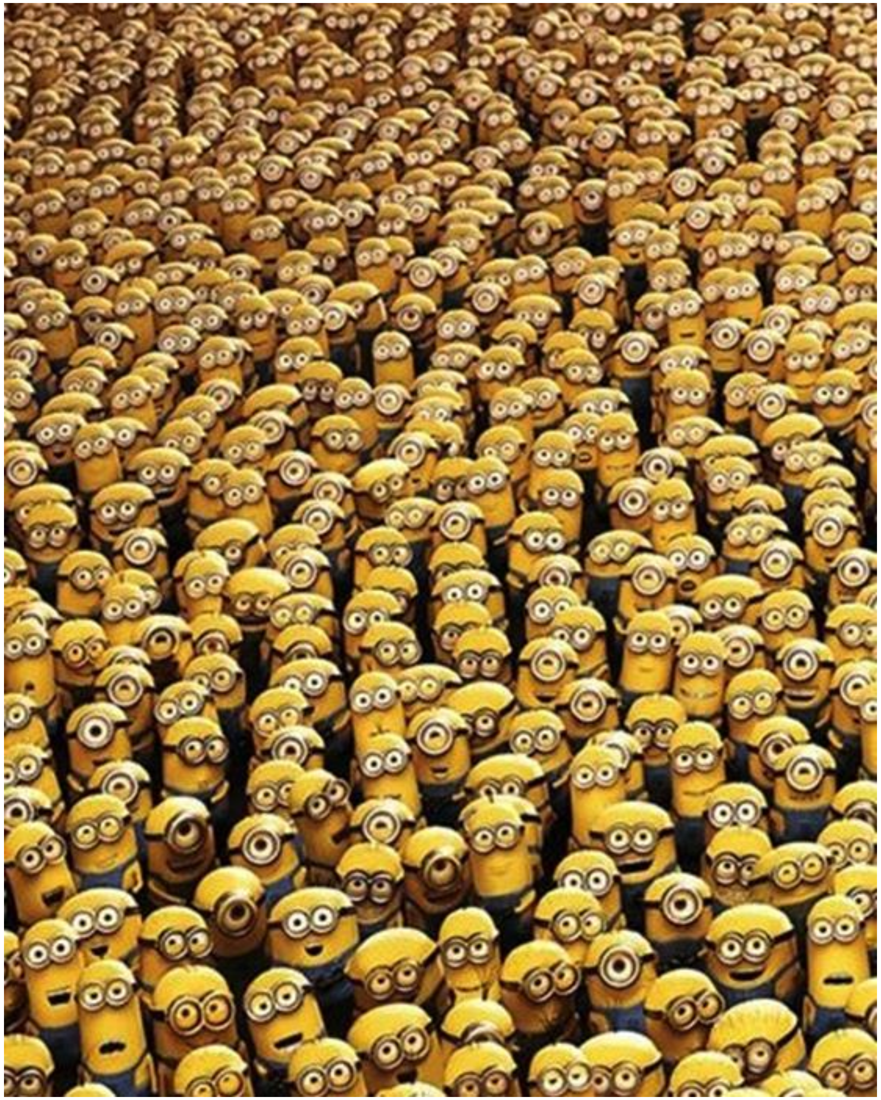
# Human Nature Is Not Going To Change

- 93% CISOs feel vulnerable to insider threats
- 59% worry about privileged users most
- See contractors/service providers next biggest concern
- 37% feel user awareness training is failing
- Year over year 20% increase in ID/Med ID theft
- Traditional audit methods are failing right and left
- Behavioral monitoring is the answer

# Innovation Will Not Slow Down

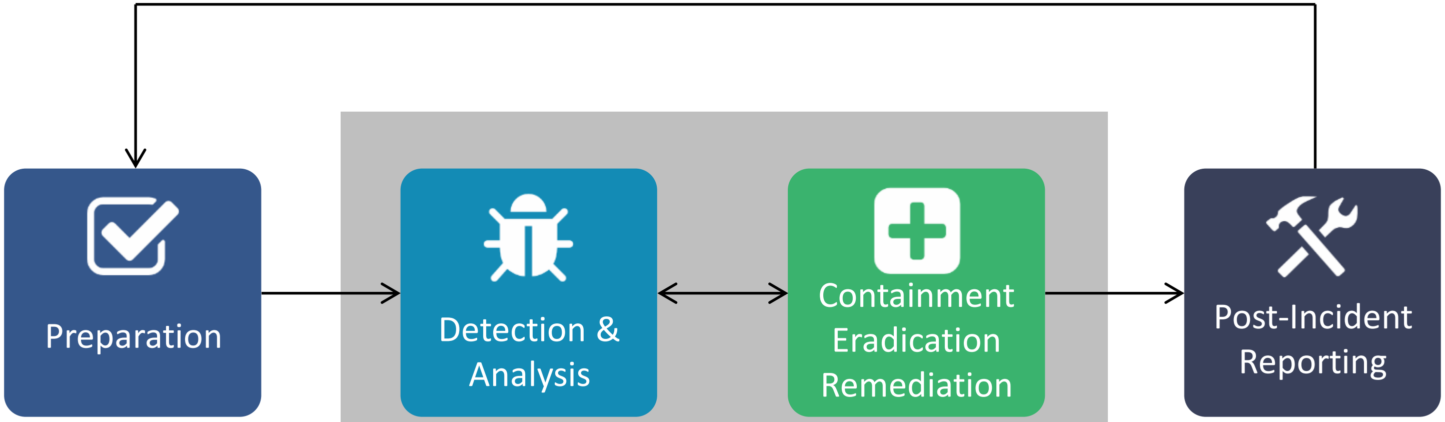
- Mobile technologies (BYOD)
- Networked medical devices
- Cloud and SaaS solutions
- Big data
- Wearable technologies
- Social media
- Home monitors
- *Whatever is next…*

# It’s Always Been About People



- Awareness must be raised at all levels:
  - Workforce
  - IT Staff
  - IRM Members
  - Executives
  - Board
- New approaches that focus on interaction, role play, exercise, simulation, etc.

# Organization & Practice Are Critical



**Preparation**

- Remove or reduce access
- Change all credentials
- Freeze changes
- Control access to physical and virtual backups
- Need current inventory

**Detection & Analysis**

- Collect current system state of all assets for comparison
- Move collected data to secure location

**Containment Eradication Remediation**

- Collect reference masters for configurations
- If not – create known best practice state
- Compare the known good with current state

**Post-Incident Reporting**

- Isolate/remove compromised systems
- Revise configs
- Redeploy
- Save copies of current state, log data
- Inform

> Life is about timing. – Carl Lewis
>
> So is breach mitigation – Mac McMillan

# Short Term Demand Outpaces Supply

- Nearly half have of all entities do not have a full-time CISO or information security manager
- Current estimates place shortage of CISOs at 1.5M
- Education & Training vehicles increasing, but time still a factor
- Short term reliance on external support is critical

# Technology Is An Imperative

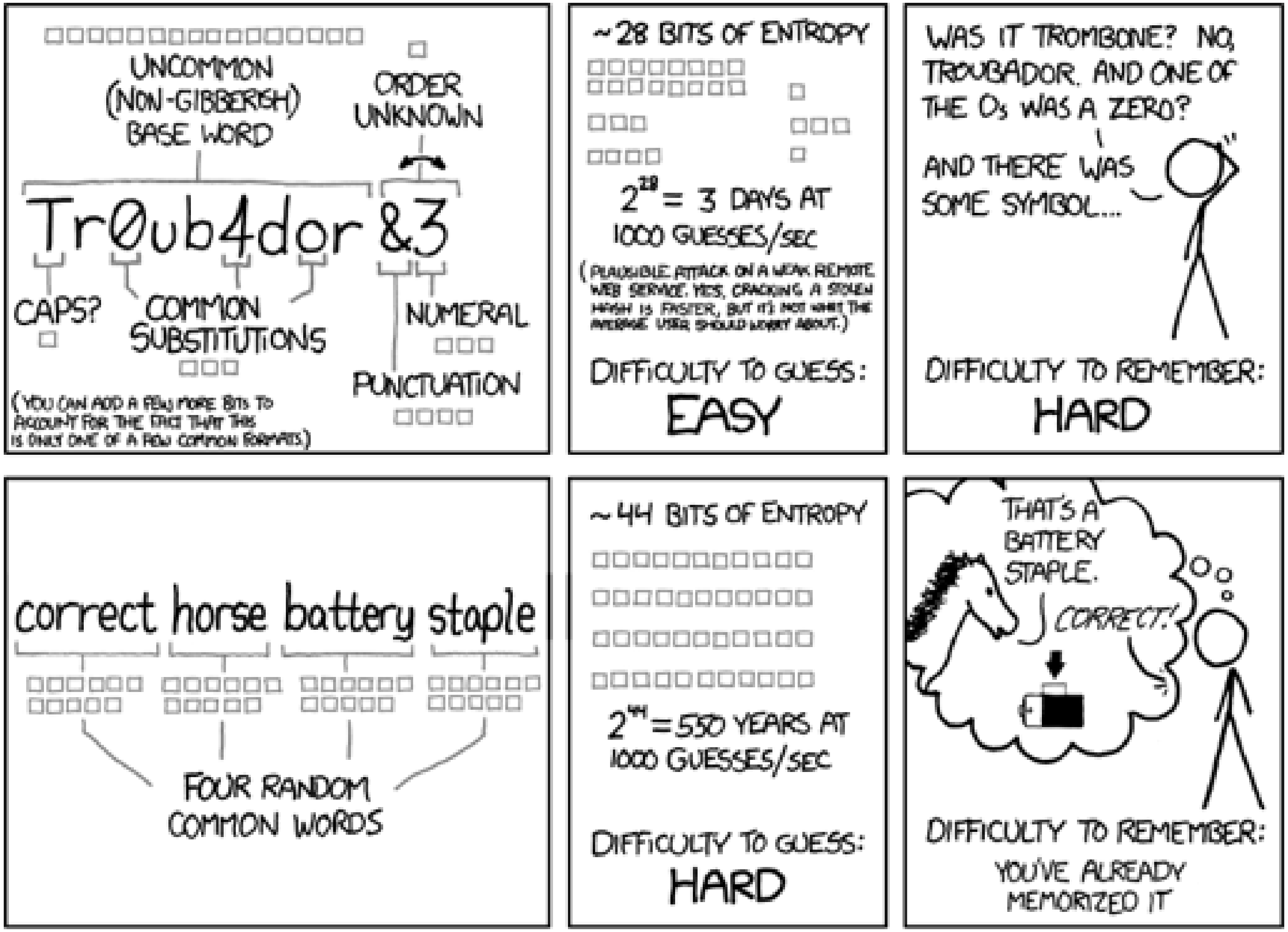
- The calibrated eyeball was never designed to read and comprehend 4,000 events per second, or 300 logs per minute or search 40 terabytes of data …
- Over 400M new malware a year, a new zero day attack every week, 3000% increase in Ransomware, automated attack tools…
- Thousands of systems, connections, employees and relationships creating 10s of millions of log events per month...
- Many healthcare organizations today don't know if they have been subject to a breach; basically, they don't know what they don't know…

# Need To Strengthen Your Defenses

- ***Improve the perimeter:*** remote access connections, firewalls/UTM, IPS, web apps, sandboxing, SaaS & public/private clouds
- ***Focus on malware detection:*** secure email gateways and secure web gateways
- ***Reinforce endpoint detection:*** admin privileges, regular testing, anti-virus, anti-malware, host based IPS, include IoT devices
- ***Automate audit/monitoring:*** dedicated SOC, enhanced SIEM, behavioral analysis
- ***Step up IR capabilities:*** define process, train members, establish contacts, track & learn, share intelligence
- ***Threat deception:*** use technologies that deceive/divert, endpoints, applications, data, identity and infrastructure

With motivation, the right equipment, the right training and timely execution ***YOU*** can stop the threat.

# Make Basics A Priority Again


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS: EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS: HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

# Compliance Is Not The Answer

- HHS Security & Privacy guidance does not fully address the important controls outlined in federal guidance.
- HHS guidance does not fully align with the NIST cybersecurity framework.

# Questions

Questions?

Mac McMillan

mac.mcmillan@cynergistek.com

512.405.8555

@mmcmillan07