RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN ELEMENT

SESSION ID: **HUM-T08**

Leading Change: Building a Security Culture of Protect, Detect & Respond

Lance Spitzner

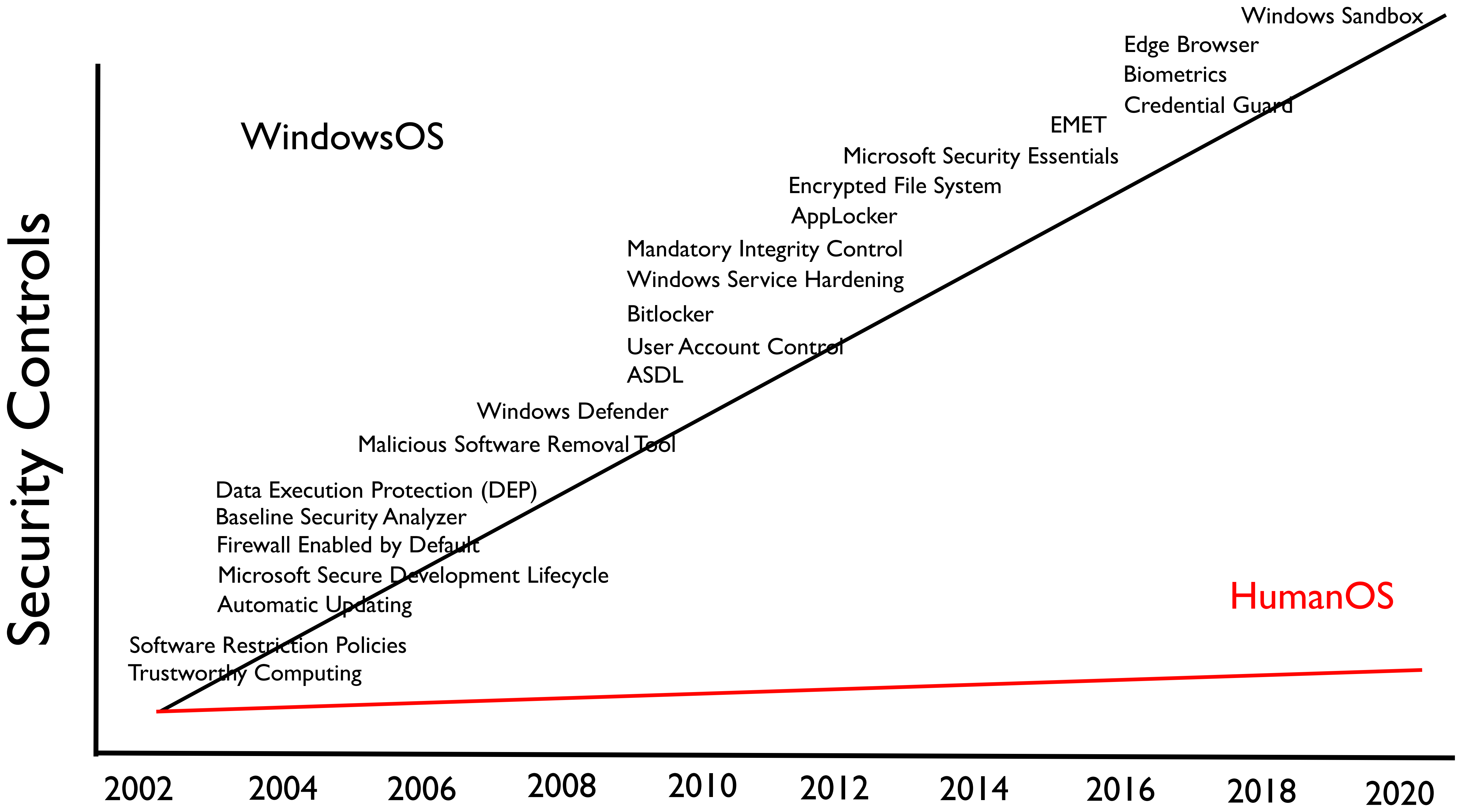
Director, SANS Security Awareness
lspitzner@sans.org
@lspitzner

#RSAC

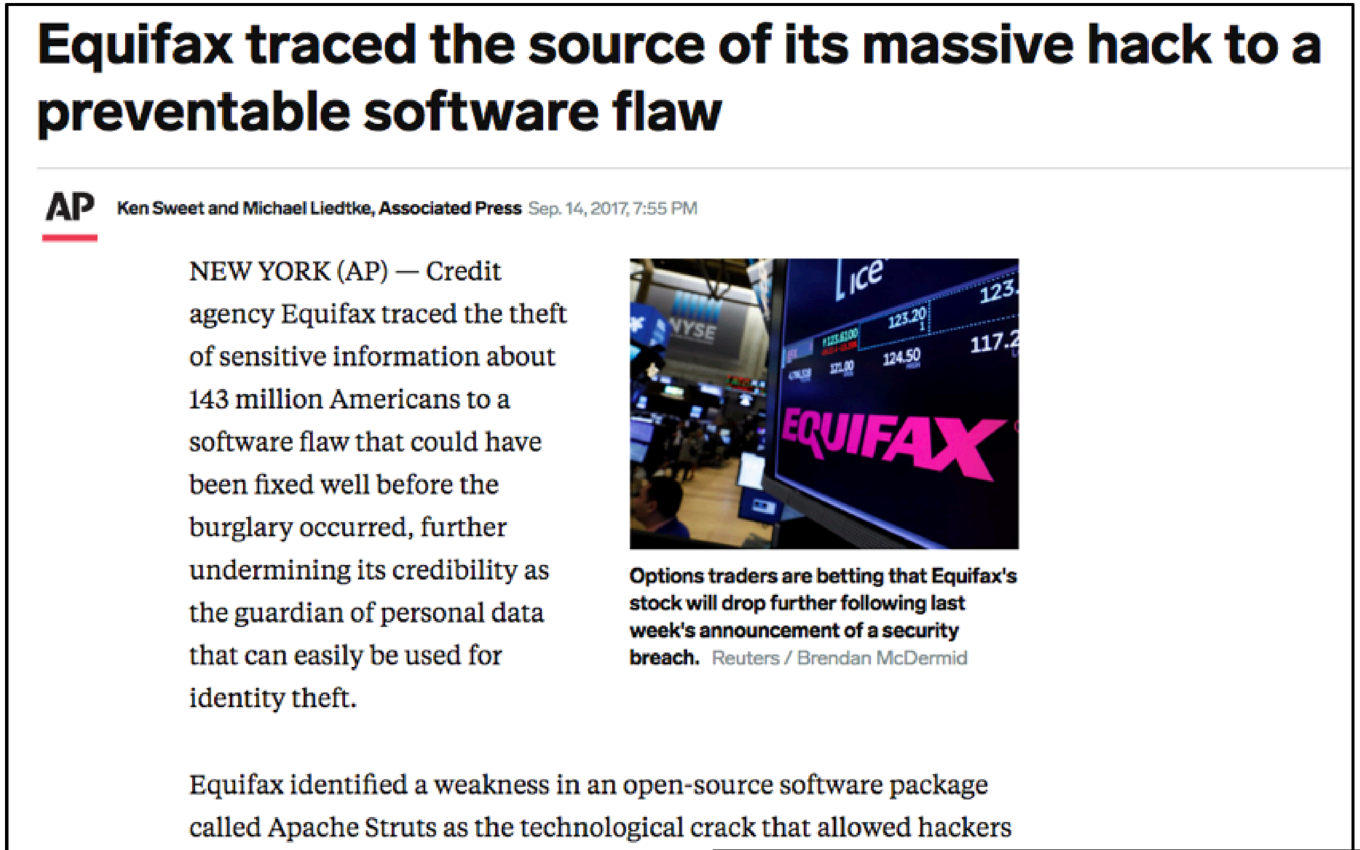
The Problem

You can‘t patch stupid

Go look in the mirror


Security Controls
WindowsOS
Windows Sandbox
Edge Browser
Biometrics
Credential Guard
EMET
Microsoft Security Essentials
Encrypted File System
AppLocker
Mandatory Integrity Control
Windows Service Hardening
Bitlocker
User Account Control
ASDL
Windows Defender
Malicious Software Removal Tool
Data Execution Protection (DEP)
Baseline Security Analyzer
Firewall Enabled by Default
Microsoft Secure Development Lifecycle
Automatic Updating
Software Restriction Policies
Trustworthy Computing
HumanOS
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020

People are not the weakest link, they are the primary attack vector



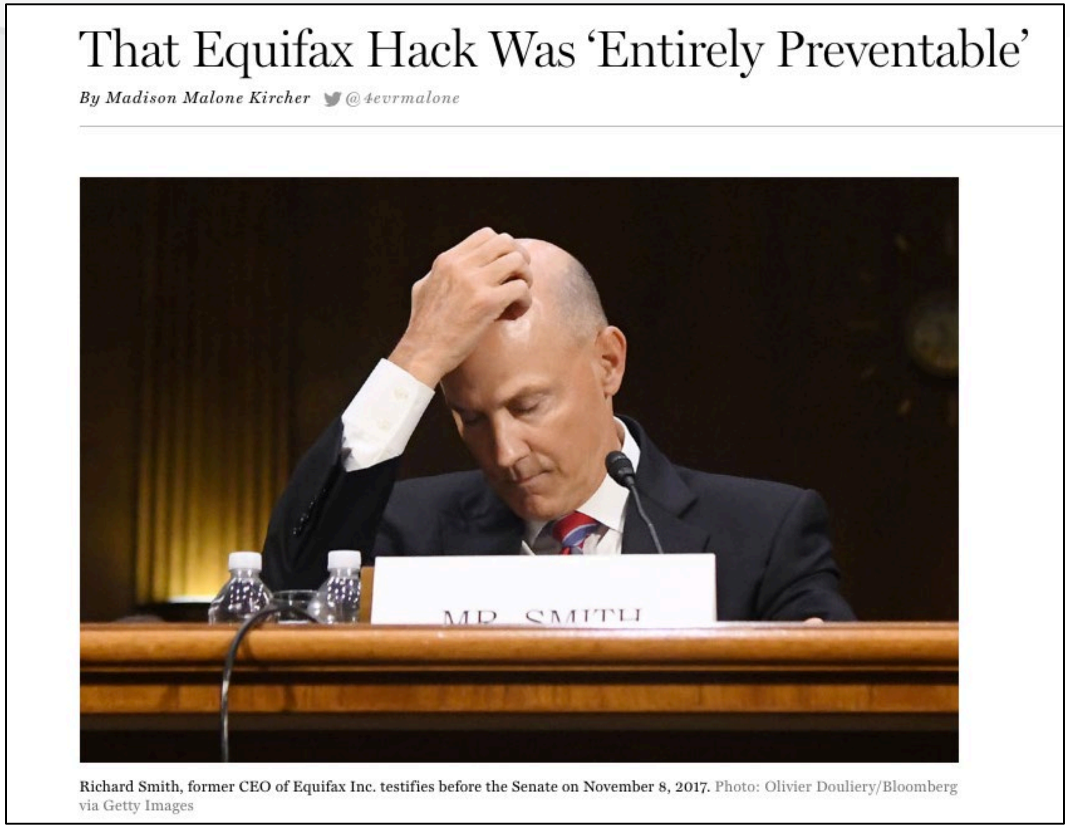
Equifax traced the source of its massive hack to a preventable software flaw

AP Ken Sweet and Michael Liedtke, Associated Press Sep. 14, 2017, 7:55 PM

NEW YORK (AP) — Credit agency Equifax traced the theft of sensitive information about 143 million Americans to a software flaw that could have been fixed well before the burglary occurred, further undermining its credibility as the guardian of personal data that can easily be used for identity theft.

Options traders are betting that Equifax's stock will drop further following last week's announcement of a security breach. Reuters / Brendan McDermid

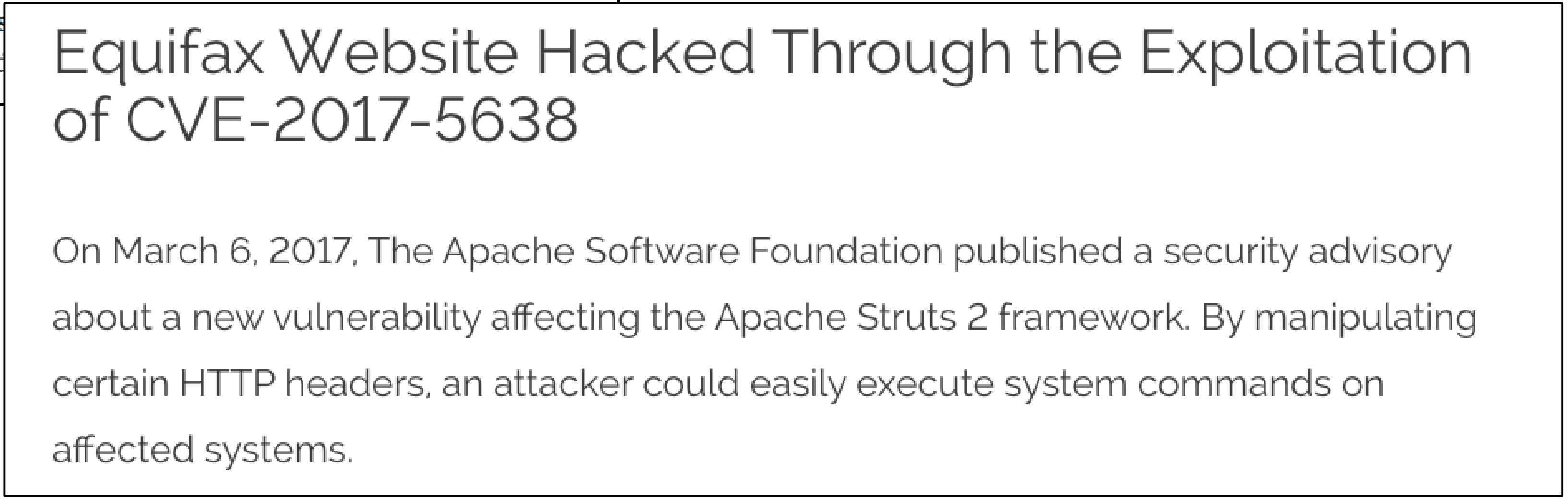
Equifax identified a weakness in an open-source software package called Apache Struts as the technological crack that allowed hackers to heist Social Security numbers, birthdates
names from a massive database maintained



That Equifax Hack Was 'Entirely Preventable'

By Madison Malone Kircher *@4evrmalone*

Richard Smith, former CEO of Equifax Inc. testifies before the Senate on November 8, 2017. Photo: Olivier Douliery/Bloomberg via Getty Images

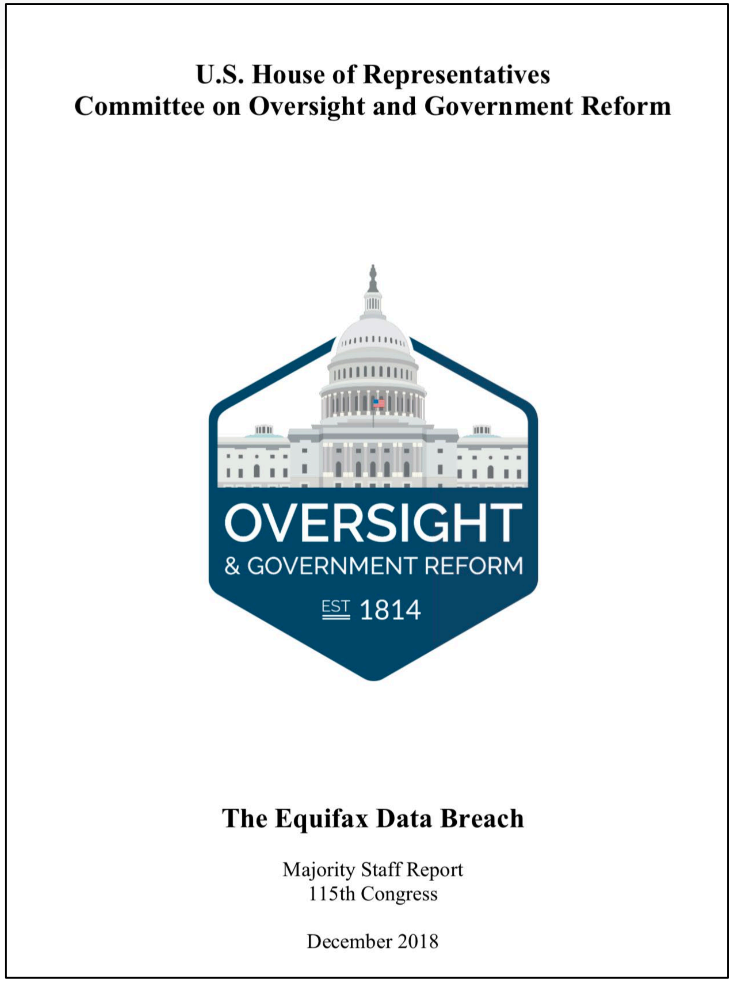


Equifax Website Hacked Through the Exploitation of CVE-2017-5638

On March 6, 2017, The Apache Software Foundation published a security advisory about a new vulnerability affecting the Apache Struts 2 framework. By manipulating certain HTTP headers, an attacker could easily execute system commands on affected systems.

2018 Congressional Report

- Apache Struts Vulnerability was a symptom of a far greater problem
- Equifax was far more dysfunctional than thought, biggest issues were people / culture



U.S. House of Representatives
Committee on Oversight and Government Reform

The Equifax Data Breach

Majority Staff Report
115th Congress

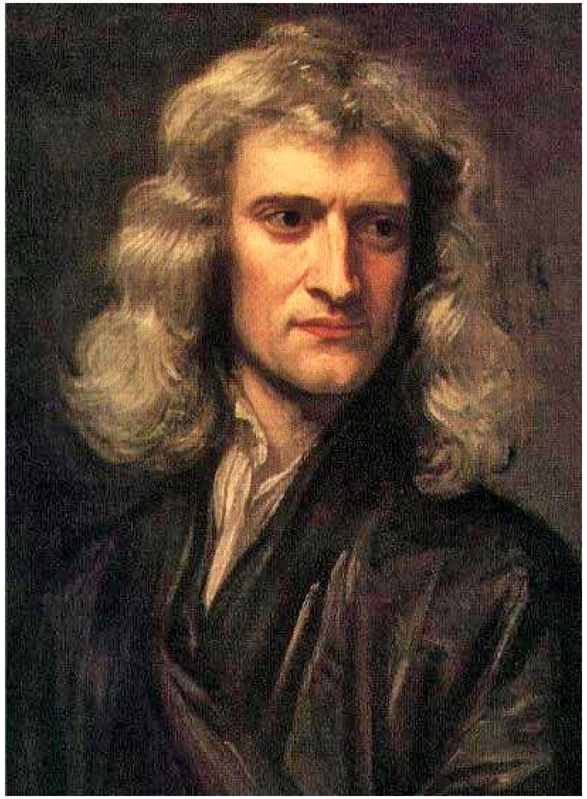
December 2018

The Solution

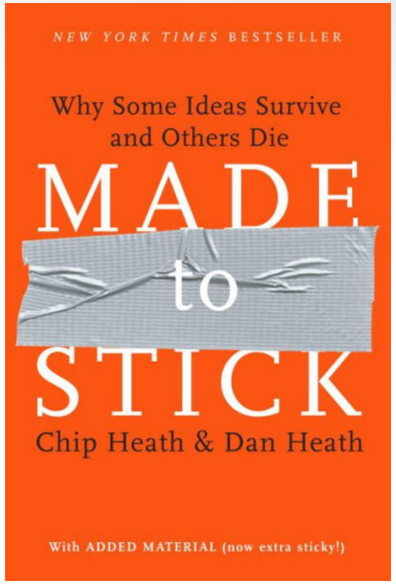
Newtons First Law

An object at rest remains at rest, or if in motion, remains in motion at a constant velocity unless acted on by a net external force.

$$F = ma$$



SKOLNICK



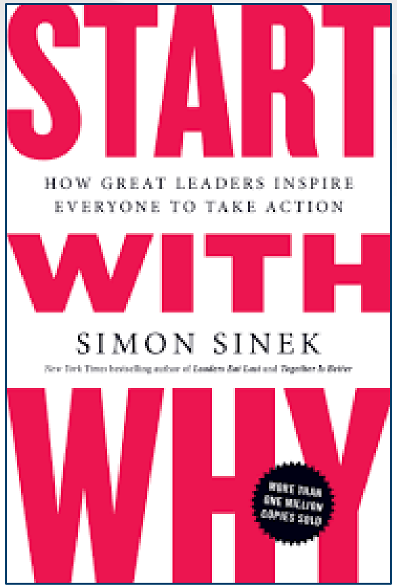
NEW YORK TIMES BESTSELLER

Why Some Ideas Survive and Others Die

MADE to STICK

Chip Heath & Dan Heath

With ADDED MATERIAL (now extra sticky!)



START

HOW GREAT LEADERS INSPIRE EVERYONE TO TAKE ACTION

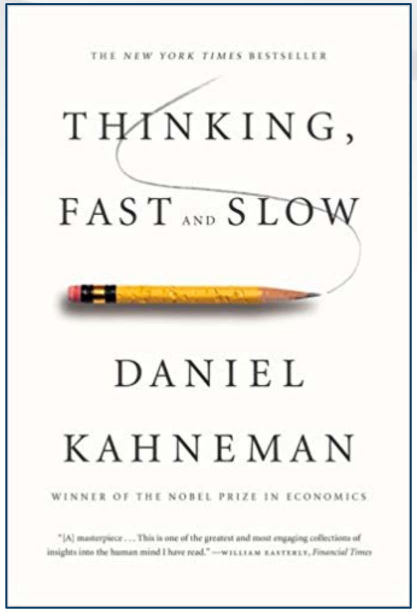
WITH

SIMON SINEK

New York Times bestselling author of Leaders Eat Last and Together Is Better

WHY

MORE THAN ONE MILLION COPIES SOLD



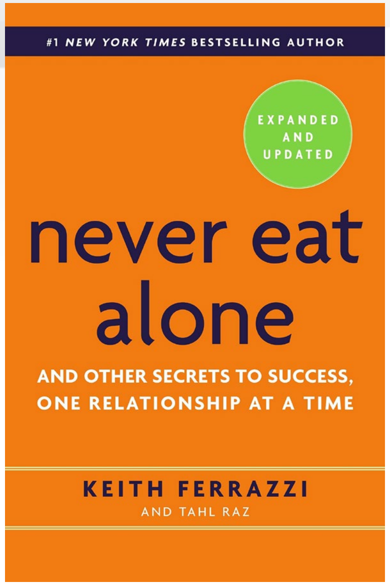
THE NEW YORK TIMES BESTSELLER

THINKING, FAST AND SLOW

DANIEL KAHNEMAN

WINNER OF THE NOBEL PRIZE IN ECONOMICS

"[A] masterpiece . . . This is one of the greatest and most engaging collections of insights into the human mind I have read." —WILLIAM EASTERLY, *Financial Times*



#1 *NEW YORK TIMES* BESTSELLING AUTHOR

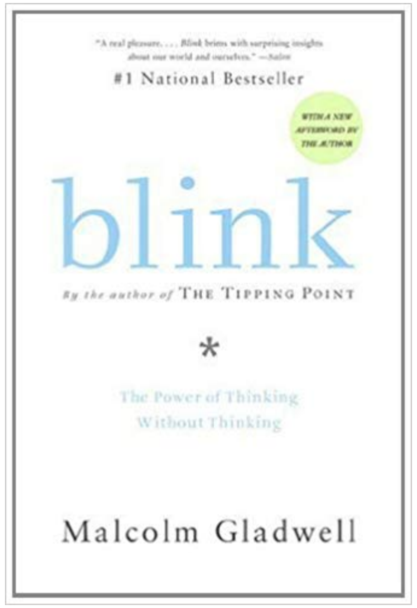
EXPANDED AND UPDATED

never eat alone

AND OTHER SECRETS TO SUCCESS, ONE RELATIONSHIP AT A TIME

KEITH FERRAZZI

AND TAHL RAZ



"A real pleasure. . . . *Blink* brims with surprising insights about our world and ourselves." —*Salon*

#1 National Bestseller

WITH A NEW AFTERWORD BY THE AUTHOR

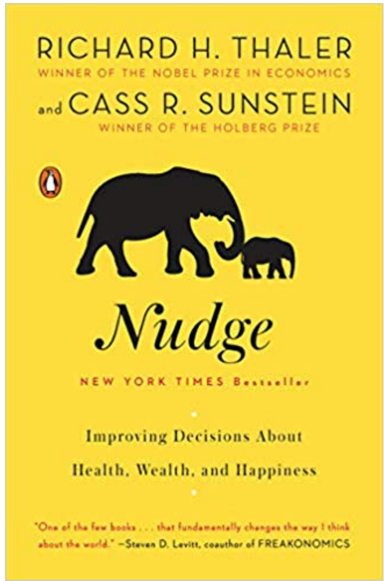
blink

By the author of THE TIPPING POINT

*

The Power of Thinking Without Thinking

Malcolm Gladwell



RICHARD H. THALER

WINNER OF THE NOBEL PRIZE IN ECONOMICS

and CASS R. SUNSTEIN

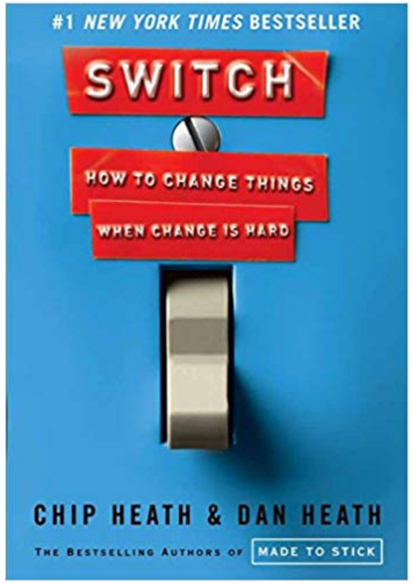
WINNER OF THE HOLBERG PRIZE

Nudge

NEW YORK TIMES Bestseller

Improving Decisions About Health, Wealth, and Happiness

"One of the few books . . . that fundamentally changes the way I think about the world." —Steven D. Levitt, coauthor of FREAKONOMICS



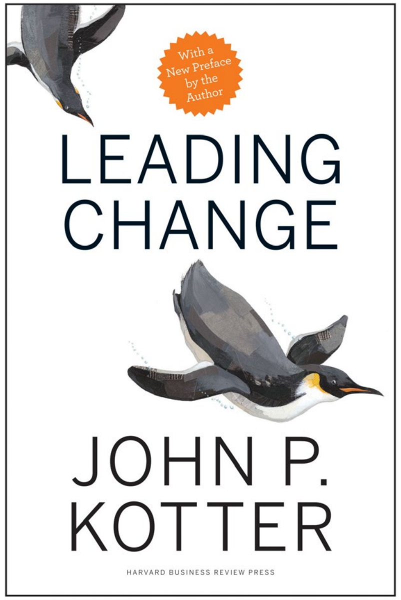
#1 *NEW YORK TIMES* BESTSELLER

SWITCH

HOW TO CHANGE THINGS WHEN CHANGE IS HARD

CHIP HEATH & DAN HEATH

THE BESTSELLING AUTHORS OF MADE TO STICK

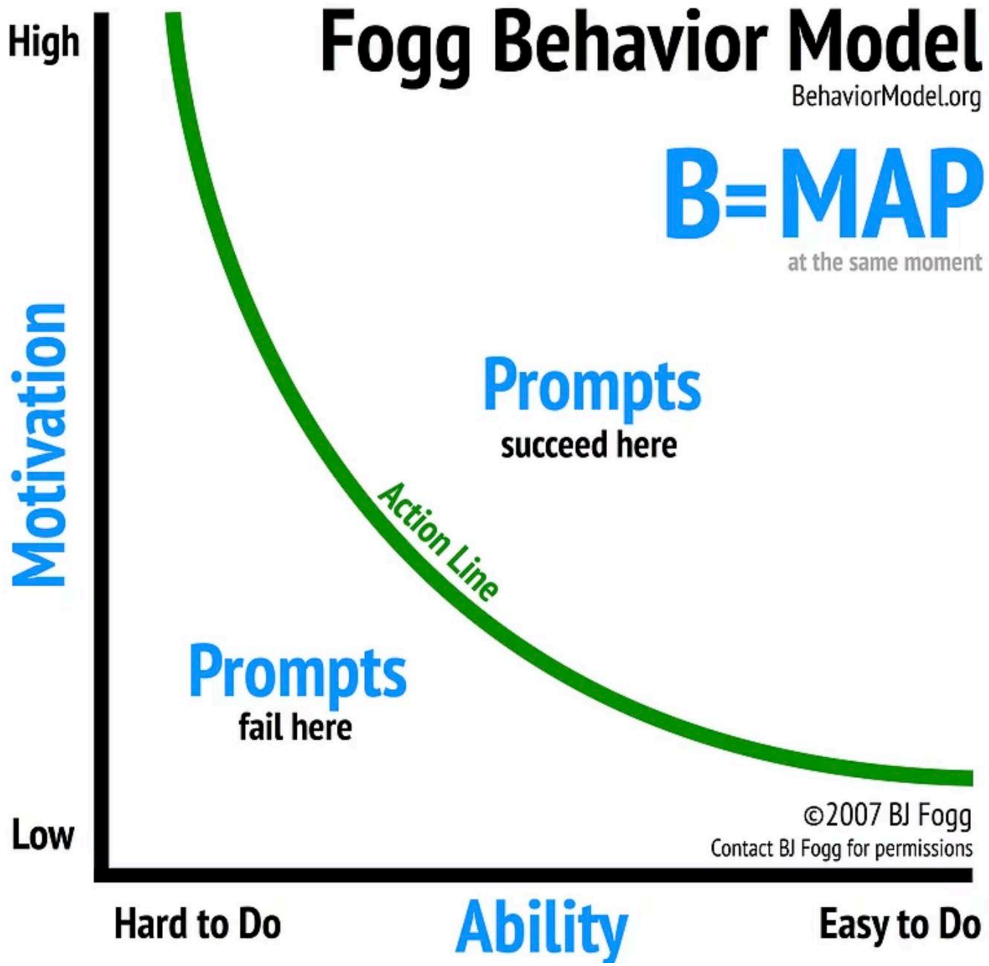


With a New Preface by the Author

LEADING CHANGE

JOHN P. KOTTER

HARVARD BUSINESS REVIEW PRESS



A	Awareness of the need for change
D	Desire to support the change
K	Knowledge of how to change
A	Ability to exhibit the change
R	Reinforcement to make change stick

KTREAT

Daniel Khaneman

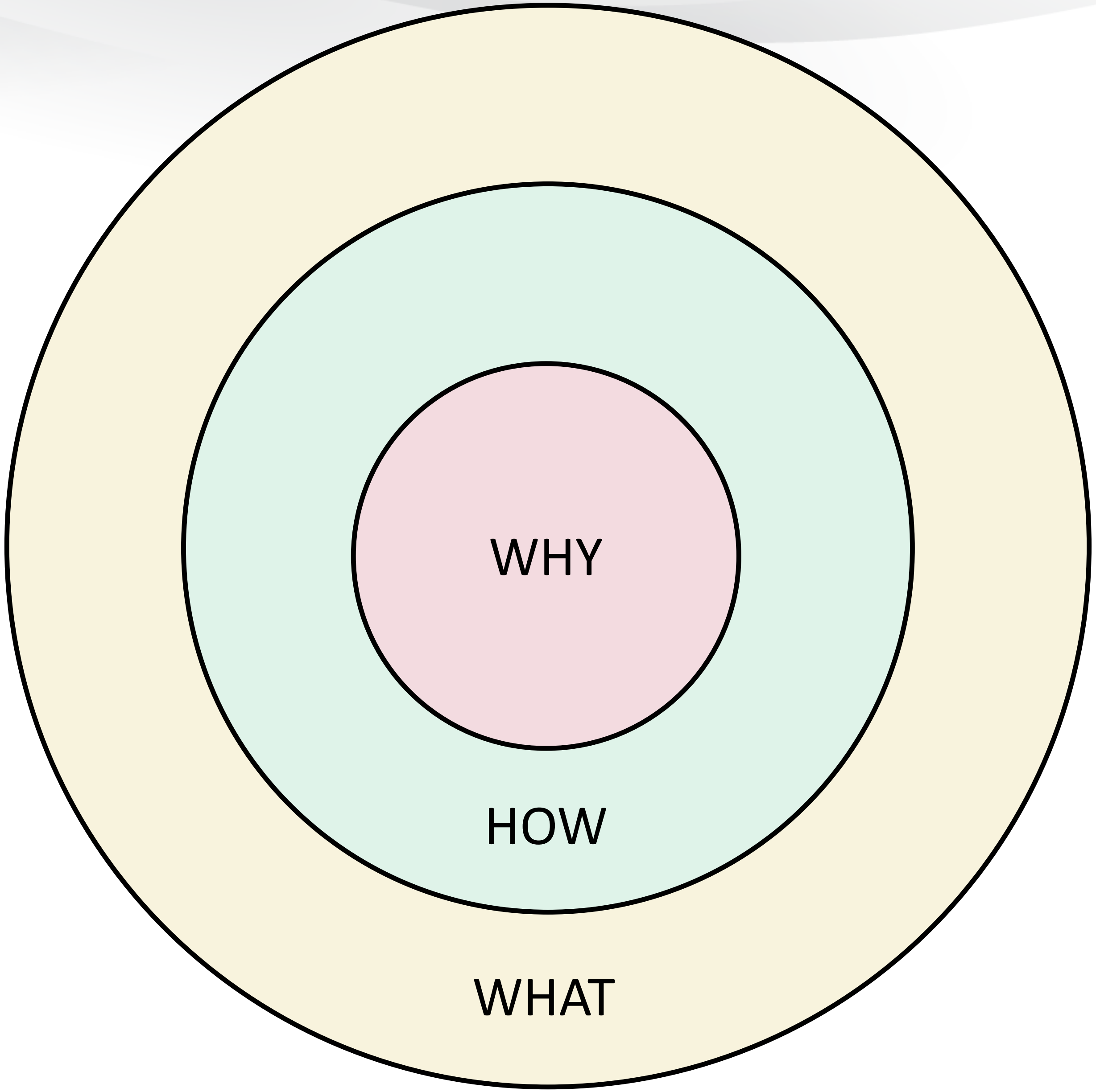
- A baseball bat and ball cost a total of $1.10
- The bat costs $1 more than the ball

How much is the ball?

Motivation

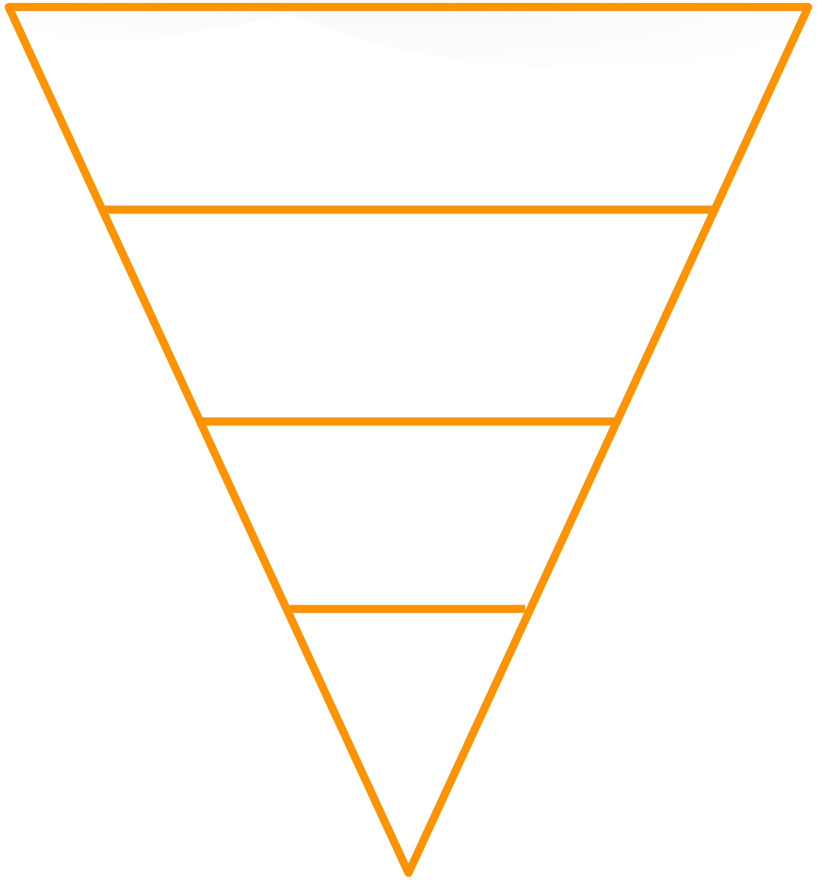
Ability

Start With Why
-
Simon Sinek



AIDA Marketing Model

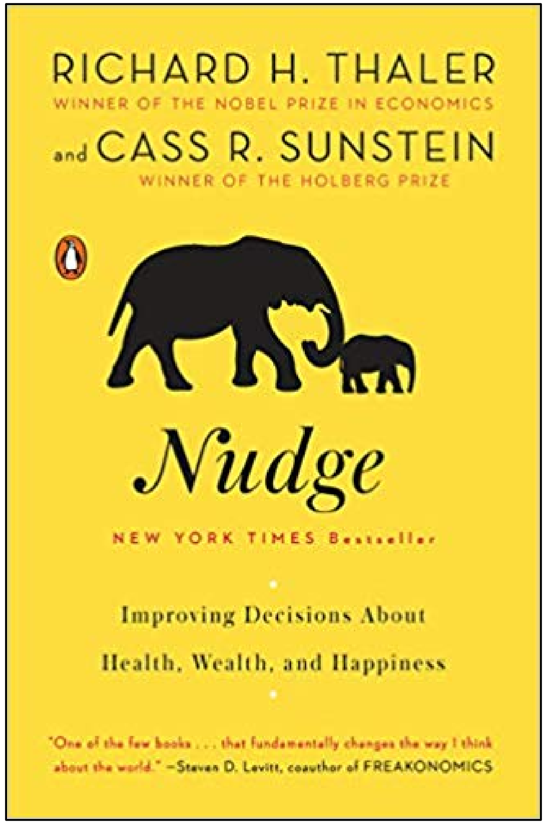
- Attention
- Interest
- Desire
- Action

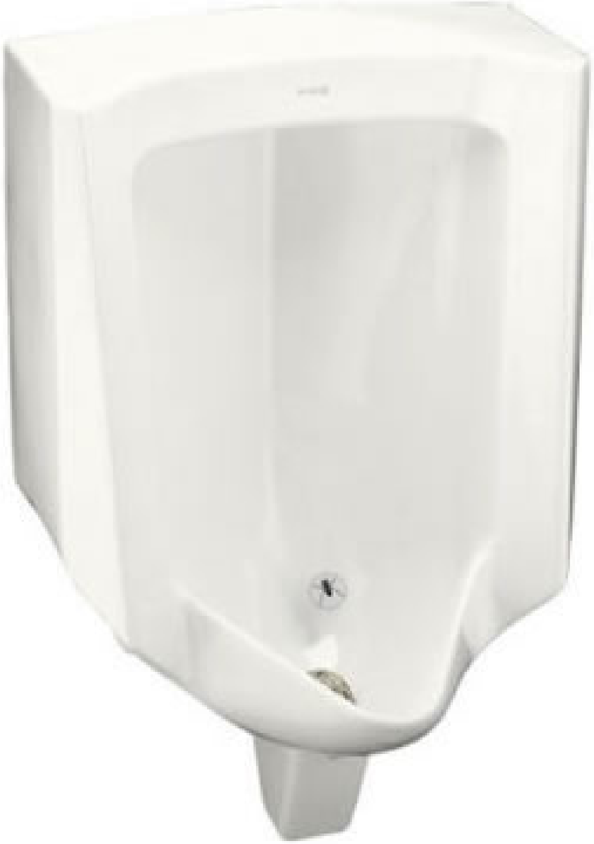


Motivation

Ability

Choice Architect


RICHARD H. THALER
WINNER OF THE NOBEL PRIZE IN ECONOMICS
and CASS R. SUNSTEIN
WINNER OF THE HOLBERG PRIZE
Nudge
NEW YORK TIMES Bestseller
Improving Decisions About
Health, Wealth, and Happiness
"One of the few books . . . that fundamentally changes the way I think about the world." —Steven D. Levitt, coauthor of FREAKONOMICS



Ability: Simplify & Train

- Simplify security
  - Reduce or eliminate policies / procedures
  - Simplify policies or procedures
  - Communicate in their terms, not yours
- Train and enable people
  - Provide training people need to be successful
  - Provide tools that make their jobs simpler

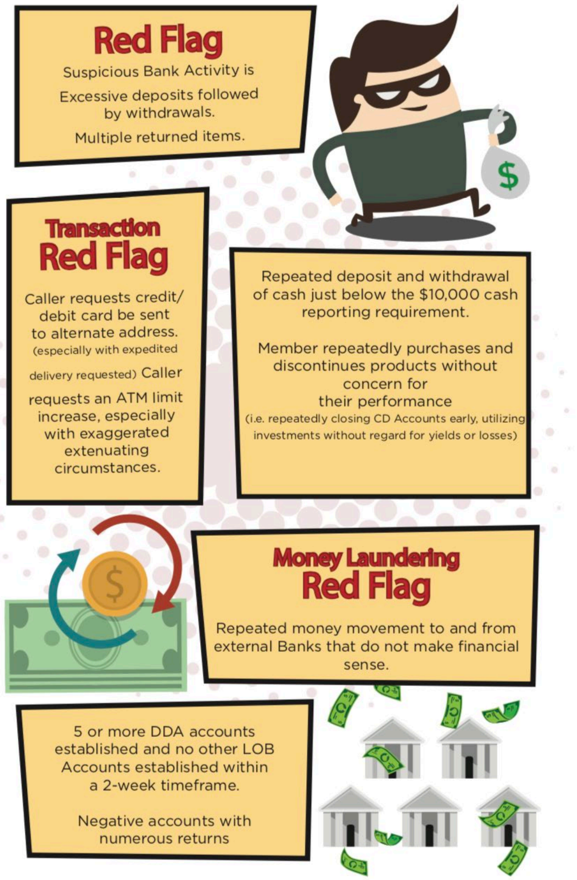
Painful Password Policies

- Every password must have a symbol, number, upper case and lower case
- Change it every ninety days
- Never write your passwords down
- Every account must have a unique password

Simplifying Passwords

1. Can we eliminate outdated or painful policies?
   - *Kill password expiration*
2. Can we replace the policies with technology?
   - *Multifactor authentication*
   - *Single Sign-On*
   - *Biometrics*
3. Can the policies be simplified?
   - *Replace complexity with passphrases*
4. Can we provide tools that simplify the process?
   - *Provide and train on Password Managers*

ENTERPRISE SECURITY GROUP
Approved by USAA
ESG COMICS GROUP ¢25
THE FRAUD FIGHTER PROGRAM
USAA Enterprise Security Group
ESG
ALWAYS VIGILANT
123 456 789 012



Red Flag

Suspicious Bank Activity is

Excessive deposits followed by withdrawals.

Multiple returned items.

Transaction Red Flag

Caller requests credit/ debit card be sent to alternate address. (especially with expedited delivery requested) Caller requests an ATM limit increase, especially with exaggerated extenuating circumstances.

Repeated deposit and withdrawal of cash just below the $10,000 cash reporting requirement.

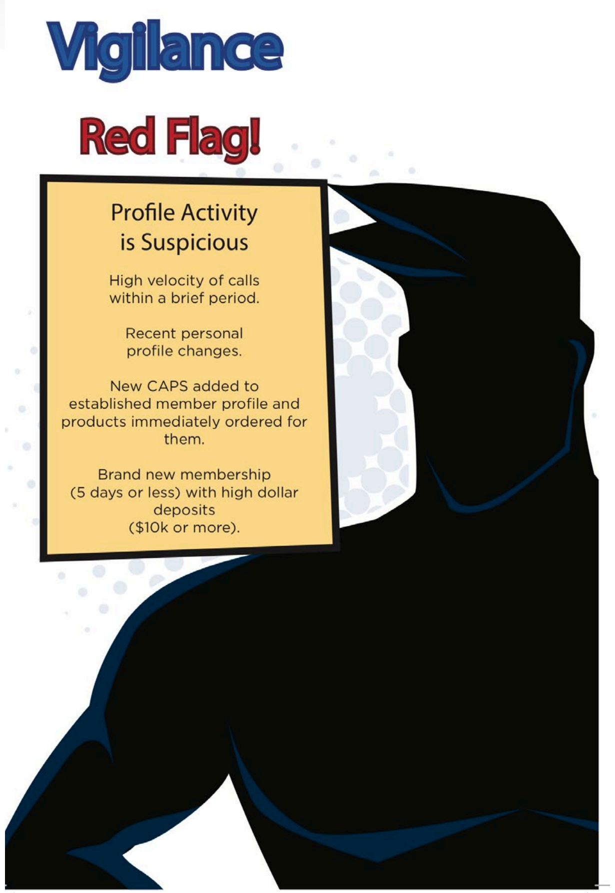
Member repeatedly purchases and discontinues products without concern for their performance (i.e. repeatedly closing CD Accounts early, utilizing investments without regard for yields or losses)

Money Laundering Red Flag

Repeated money movement to and from external Banks that do not make financial sense.

5 or more DDA accounts established and no other LOB Accounts established within a 2-week timeframe.

Negative accounts with numerous returns



Vigilance

Red Flag!

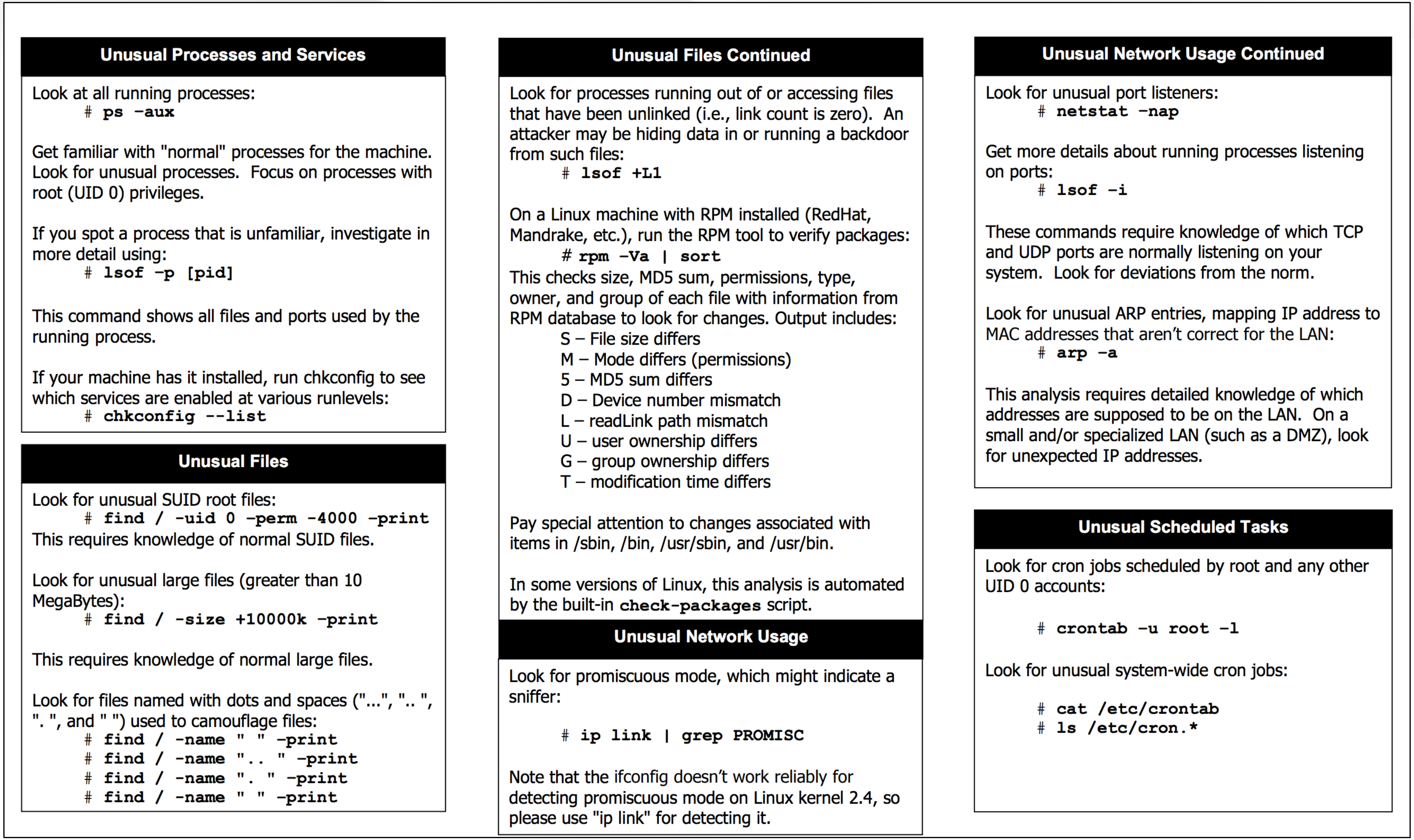
Profile Activity is Suspicious

High velocity of calls within a brief period.

Recent personal profile changes.

New CAPS added to established member profile and products immediately ordered for them.

Brand new membership (5 days or less) with high dollar deposits ($10k or more).



Unusual Processes and Services

Look at all running processes:

```
    # ps -aux
```

Get familiar with "normal" processes for the machine. Look for unusual processes. Focus on processes with root (UID 0) privileges.

If you spot a process that is unfamiliar, investigate in more detail using:

```
    # lsof -p [pid]
```

This command shows all files and ports used by the running process.

If your machine has it installed, run chkconfig to see which services are enabled at various runlevels:

```
    # chkconfig --list
```

Unusual Files

Look for unusual SUID root files:

```
    # find / -uid 0 -perm -4000 -print
```

This requires knowledge of normal SUID files.

Look for unusual large files (greater than 10 MegaBytes):

```
    # find / -size +10000k -print
```

This requires knowledge of normal large files.

Look for files named with dots and spaces ("...", ".. ", ". ", and " ") used to camouflage files:

```
    # find / -name " " -print
    # find / -name ".. " -print
    # find / -name ". " -print
    # find / -name " " -print
```

Unusual Files Continued

Look for processes running out of or accessing files that have been unlinked (i.e., link count is zero). An attacker may be hiding data in or running a backdoor from such files:

```
    # lsof +L1
```

On a Linux machine with RPM installed (RedHat, Mandrake, etc.), run the RPM tool to verify packages:

```
    # rpm -Va | sort
```

This checks size, MD5 sum, permissions, type, owner, and group of each file with information from RPM database to look for changes. Output includes:

S – File size differs
M – Mode differs (permissions)
5 – MD5 sum differs
D – Device number mismatch
L – readLink path mismatch
U – user ownership differs
G – group ownership differs
T – modification time differs

Pay special attention to changes associated with items in /sbin, /bin, /usr/sbin, and /usr/bin.

In some versions of Linux, this analysis is automated by the built-in **check-packages** script.

Unusual Network Usage

Look for promiscuous mode, which might indicate a sniffer:

```
    # ip link | grep PROMISC
```

Note that the ifconfig doesn't work reliably for detecting promiscuous mode on Linux kernel 2.4, so please use "ip link" for detecting it.

Unusual Network Usage Continued

Look for unusual port listeners:

```
    # netstat -nap
```

Get more details about running processes listening on ports:

```
    # lsof -i
```

These commands require knowledge of which TCP and UDP ports are normally listening on your system. Look for deviations from the norm.

Look for unusual ARP entries, mapping IP address to MAC addresses that aren't correct for the LAN:

```
    # arp -a
```

This analysis requires detailed knowledge of which addresses are supposed to be on the LAN. On a small and/or specialized LAN (such as a DMZ), look for unexpected IP addresses.

Unusual Scheduled Tasks

Look for cron jobs scheduled by root and any other UID 0 accounts:

```
    # crontab -u root -l
```

Look for unusual system-wide cron jobs:

```
    # cat /etc/crontab
    # ls /etc/cron.*
```

Applying Lessons Learned

- Start with WHY for any security initiative.
- Create a security awareness / engagement position – someone with soft skills.
- Partner with or have someone from Communications / Marketing assigned to your security team
- Review your most complex policies or behaviors, how you can you simplify them?

If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.

Bruce Schneier

lspitzner@sans.org