RSAConference2015
San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-T07R

News Flash: Some Things Actually Do Work in Security!!!

John Pescatore

Director, Emerging Security Trends
SANS Institute
@John_Pescatore


Uber Driver Data Exposed
Target Breach: $162M
Sony Email Hacked
Largest Breach Ever…
Eurosystem Compromised
China! NSA!
Anthem Exposes 80M
Chick-fil-A Gets Fileted


Tweets
Following
Followers
Favorites
Lists
Tweet to Twitter
@twitter
Similar to Twitter
Engadget @engadget
Follow
Laurence Georgiou @UberGeorgiou
Follow
Adele @OfficialAdele
Follow
© 2012 Twitter About Help Terms Privacy
Blog Status Apps Resources Jobs
Advertisers Businesses Media Developers
1,488
14,998,991
FOLLOWERS
Follow
Twitter @twitter
The pulse of your city - Trends are now a
around the world. blog.twitter.com/2012/1
Expand
Twitter Government @gov
Today at 2pm ET President Obama will be twe
@whitehouse to answer #my2k questions abo
twitter.com/whitehouse/sta...
Retweeted by Twitter
View tweet
Twitter Good @TwitterGood
Online tools that make Sandy fundraising easier: cbsn.ws/WcyVcR
NEWS
Recession
Credit Crunch
Economic Crisis

A Short Reality Break

- Retail fraud averages about 1.5% of sales
  - Target 2014 Revenue = $73B, so about $1.1B of fraud
  - The online breach was big but only 15% of Target's acceptable cost of fraud
- Another way to look at it:

If Target had avoided the breach but increased shopping cart abandonment rate by 1% it would have decreased its return to shareholders.

Which is more effective at selling flood damage restoration services?

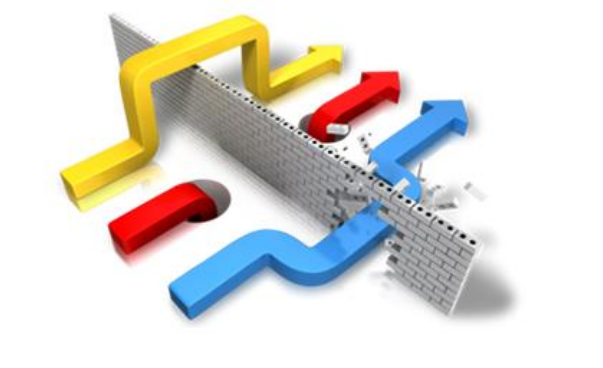
Which is more effective at selling home waterproofing services?

Which Career Are You Looking For?

What Is Your CEO Looking For?

CEO Laurence Olivier asks CISO Dustin Hoffman a simple question in 1976's "Marathon Man"

There Are a Lot of Overcome Obstacles Out There



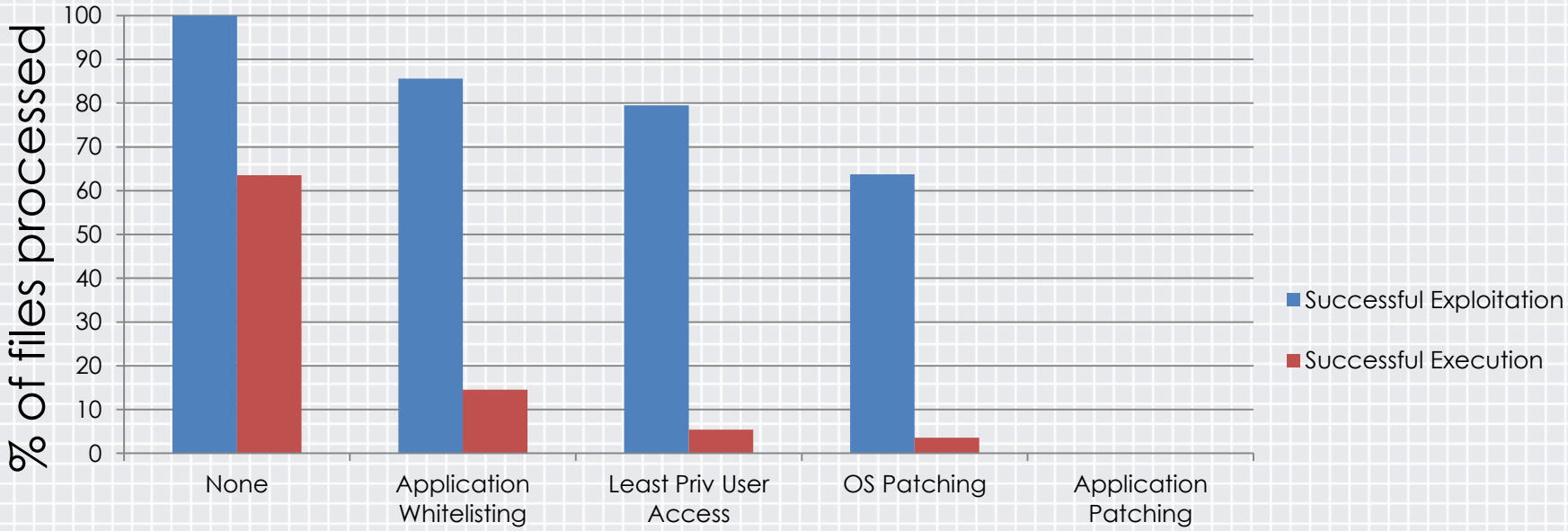
- Increase Effectiveness and Efficiency
  - Avoid more vulnerabilities
  - Block more attacks
  - Detect incidents more quickly
  - Free up budget to deal with emerging threats

Problem: Malware leading to breaches but more frequently to expensive PC re-imaging

- **Solutions that work:**
  - Lockdown
  - Network-based Advanced Threat Detection
  - Privilege Management/Whitelisting
  - Endpoint Intrusion Prevention/Containment

Australian Government
Department of Defence

Malware Vs. Top 4 Critical Controls



Cumulative security mitigation

VIRGINIA COMMONWEALTH UNIVERSITY

Advanced Threat Detection

- Problem: Typical university environment meant distributed management of desktops, lots of BYOD, high rate of malware being found on PCs.
- Solution: Network-based Advanced Threat Detection appliances (Fireeye) at Internet ingress point.
- Results:
  - Intrusion Detection Rate **increased** 46%
  - Incident rate (requiring corrective action) **decreased** 35%

Better Endpoint Security

- Problem: Financial services firm found traditional anti-viral was not able to address advanced targeted threats.
- Solution: Host based security (Invincea) on Windows PCs.
- Results:
  - Baseline average was **reimaging 4 PCs per week**
  - After deployment, **reimaging 1 PC every 3 months**
  - **Look at cheaper/free AV in the future?**

Problem: Reducing Vulnerabilities

- **Solutions that work:**
  - Spend less on the easy parts
  - Innovative application testing approaches
  - Mature and Secure Software Development Lifecycle

Reduce Cost of Vulnerability Scanning

- Problem: Healthcare Services firm was at renewal point for vulnerability scanning solution.
- Solution: Switched to Tenable Nessus/System Center
- Results:
  - **Reduced** spending by 75%
  - Able to use savings to **increase** frequency and coverage of scanning

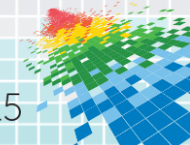
More Effective Identification of Application Vulnerabilities

- Problem: Reduce vulnerabilities in revenue-bearing applications.
- Solution: Switched from consulting engagement to “managed crowdsourced bug bounty” approach (Bugcrowd)
- Results:
  - Same spending resulted in 10x **increase** in vulnerabilities discovered
  - Testers **increased** from 2-3 to 63
  - **Higher quality/more developer-friendly** vuln info provided

aetna®

Reduce Cost and Risk of Corporate Applications

- Problem: Healthcare company needs to reduce threat exposure and bug fix costs across all corporate applications.
- Solution: Participated in Building Security In Maturity Model (Cigital) to reduce vulnerabilities in corporate apps
- Results:
  - Defect density **decreased** by 92% for high/moderate vulnerabilities
  - Apps using secure library **increased** each month
  - Threat modeling approach **reduced** resource time from 40 hours to 2
  - Overall CDLC productivity **increase** of 15% estimated



Action Steps

- Is a major transition coming?
  - Windows migration, move to SaaS, etc
  - Re-org, merger/acquisition
- Did one of your peers get breached?
- Security product refresh coming up?
- Is it time for an audit or penetration test?

Choose Where to Start

- Think like a shareholder
- Think like an attacker
- Think like a realist
- Choose a framework
  - Critical Security Controls
  - PCI Prioritization Guidelines
  - UK CyberEssentials
  - NIST/EO

Resources

- SANS What Works - http://www.sans.org/critical-security-controls/case-studies
- Critical Security Controls - http://www.counciloncybersecurity.org/critical-controls/
- PCI Prioritization Guidelines - https://www.pcisecuritystandards.org/security_standards/prioritized.php
- NSA Top Ten - https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_Top10IAMitigationStrategies_Web.pdf