Cyber Leadership:

How to Win the Battle AND the War

G. Mark Hardy, CISSP, CISM, CISA
gmhardy@nationalsecurity.com
+1 410.933.9333
@ g_mark

Agenda

- Review of the threat landscape
- How are we doing fighting back?
- Resources, strategies, and constraints
- Legislative changes for 2015
- Attacking the human
- Managing risk in a brave new world
- Leveraging expertise
- Conclusions

Review of the Threat Landscape

The Usual Suspects

- Employee errors or carelessness
  - Attack vector: phishing
- Disgruntled employees
  - Attack vector: direct alteration of systems
- Hackers (the evil kind, not me :)
  - Attack vector: malware
- Criminals / organized crime
  - Attack vector: memory scraping (card fraud)

Emerging Threats

- Advanced Persistent Threat (APT)
  - – Attack vector: low and slow
- Business disruptors
  - – Attack vector: distributed denial of service (DDOS)
- Sophisticated attackers
  - – Attack vectors: polymorphic malware; zero-day attacks

Increased Vulnerabilities

- Larger attack surface (more devices; extensive connectivity)
- Targeting through social media
  - – 60% of dating apps vulnerable to hackers*

- Increased dependence on third-party providers
  - – Think implications of Anthem data loss
- Increasing impact of unprotected vulnerabilities
  - – Damage rarely localized anymore

Ref: https://www-03.ibm.com/press/us/en/pressrelease/46023.wss

How Are We Doing Fighting Back?

Losing Numbers

- $445 billion: Annual cybercrime loss to global economy
- $16 billion: Annual credit and debit card fraud
- $11 million: Average cost to organization of successful cyber attack
- 229 days: Average time attackers go undetected
- Bottom line: We're not doing such a great job

Ref: IBM i2; Mandiant; Javelin studies

So, What’s the Winning Move?

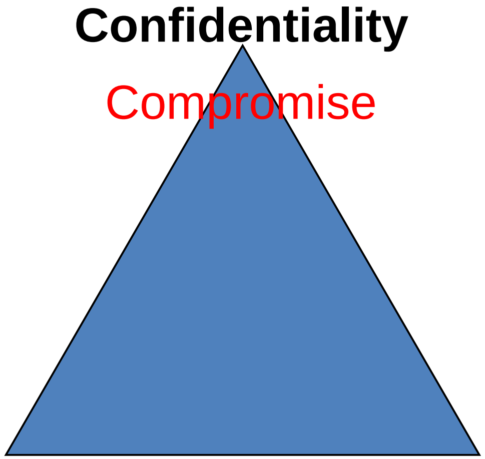
- Remember CIA? (No, not the guys on the Potomac)
- Defend confidentiality from compromise
- Defend integrity from modification
- Defend availability from denial of service (DOS)

Confidentiality
Compromise

Integrity
Modification
Availability
DOS

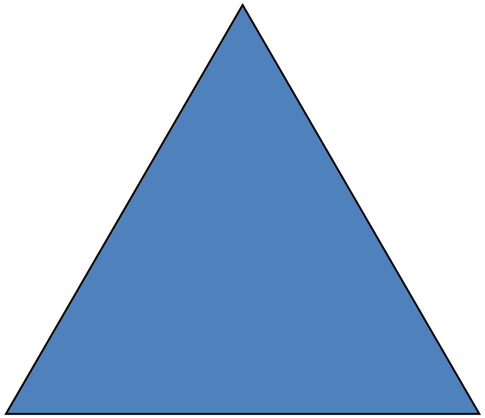
Winning at Cyber Defense

- Protect confidentiality from compromise
  - The usual:
    - Encryption
    - Access control
    - Classification
  - Often missing:
    - Egress filtering
    - Self-tracking information
  - What's the difference here?
    - Prevention vs. detection



Winning at Cyber Defense

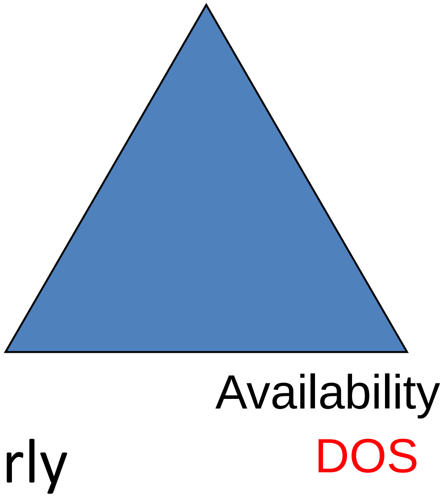
- Protect integrity from modification
  - The usual:
    - Checksums and hashes
    - Rights and privileges
    - Version control
    - Backups
  - How about:
    - Self-auditing systems
    - Decoy information (honeypots)
    - Widely distribute partial data



Integrity

Modification

Winning at Cyber Defense



- Protect availability from denial of service:
  - The usual:
    - Maintain hardware and software regularly
    - Redundancy and failover
    - High-availability; resistance to flooding
    - Disaster recovery tested and current
  - How about:
    - Hidden copies of critical systems
    - Upline filtering and interdiction
    - Hide within IPv6

We Continue to Get Pwned

Image: http://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s

We Need a Battle Plan

- Prevent
  - Robust defenses to keep attackers from gaining a foothold in our enterprises
- Detect
  - Rapid and accurate determination of the presence of an attacker or malware
- Respond
  - Decisive action that immediately blocks the threat from continuing and lowers risk

Need Adaptive Security to Succeed

- Must automate detection AND intervention
- Must share and correlate information across disparate platforms
- Customize based on user, app, and circumstance
- Must detect (and respond to) unusual or dangerous behavior
- There are many vendor solutions out there today, but that's not the point…

KNOWS 100 WAYS TO KILL PEOPLE
KNOWS 100 WAYS TO CRASH YOUR COMPUTER
S.E.A.L.
I.T.s RULE!
NAVYBROADSIDE.COM
Bacon ©2007

The Navy's most dangerous people

Image © The Broadside Blog, used with permission

By the Numbers…

- Median days attackers present before detection: 229 ↓
- Percentage of victims who detected own breach: 33 ↑
- Percentage increase in targeted attack campaigns: 91 ↔
- Number of identities exposed via breaches: 552 M ↓

- Best result: Keep the bad guys out (prevent)
- Needed result: Minimize the losses once they're in (detect and respond)
  - This is not defeatist. This is realistic.
  - If you assume you are already compromised, you have to think in an entirely new way.

Ref: https://dl.mandiant.com/EE/library/WP_M-Trends2014_140409.pdf
http://www.symantec.com/security_response/publications/threatreport.jsp

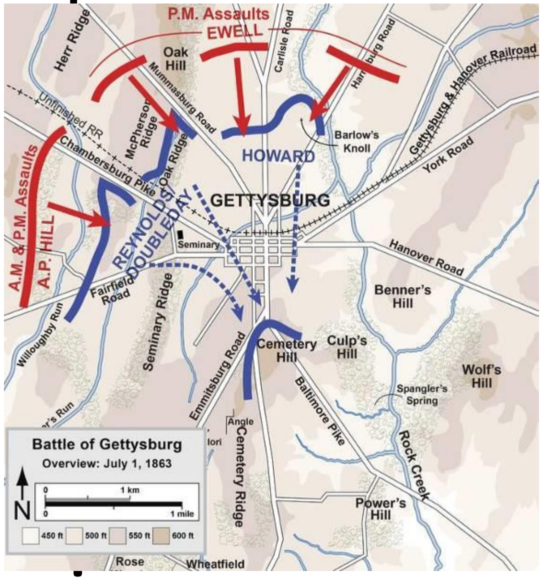
Get Smart

- You need security intelligence.
  - Battlefield commanders depend on accurate information about the opponent.
    - Threat intelligence
    - Advanced analytics
    - Expert analysis
    - Rapid response
- But you need more than intelligence to succeed…

Image public domain; source: http://en.wikipedia.org/wiki/File:DonAdams.jpg

Create Actionable Intelligence

- You can’t fight a battle with just a pile of data.
- Need to refine it:
  - – Event correlation
  - – Threat prioritization
  - – Real-time analysis
  - – Understandable reporting



- Need to be able to perform forensics:
  - – What went right? What went wrong?
  - – Use feedback loop to make better decisions.

Map by Hal Jespersen, http://www.posix.com/CW
Image source: http://en.wikipedia.org/wiki/File:Gettysburg_Battle_Map_Day1.png

Resources, Strategies, and Constraints

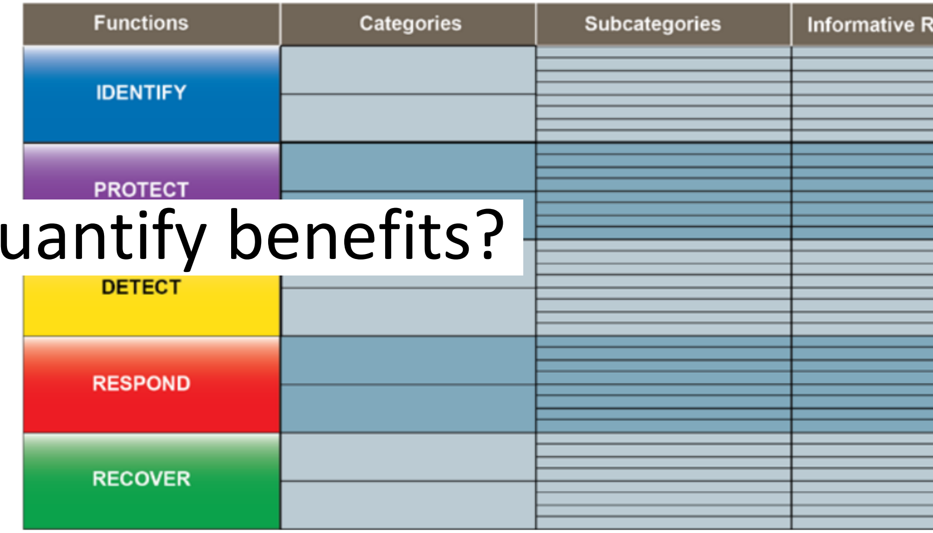
Resources and Strategies

- Security frameworks
  - U.S. Cybersecurity framework
  - COBIT (Control Objectives for Information Technology)
  - Critical Security Controls
  - FISMA (Federal Information Security Management Act)
  - ISO 27000 Series
  - NIST SP800-53 rev 4

What Do We Mean By Framework?

- Consists of standards, guidelines, and practices
- It isn't a solution, but a starting point
- Serves to organize and categorize security tasks
- Provides a common reference point

- Are you using a security framework?
  - Have you been able to quantify benefits?
    - Fewer compromises
    - Improved integrity
    - Higher availability



Functions	Categories	Subcategories	Informative R
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			

Framework Considerations

- Determine if you have compliance requirements
- Identify framework best aligned with business structure or model
- It has to be more than just a check in the box:
  - Implemented correctly, security frameworks help significantly reduce risk
- Consider impact on customers and partners

Constraints

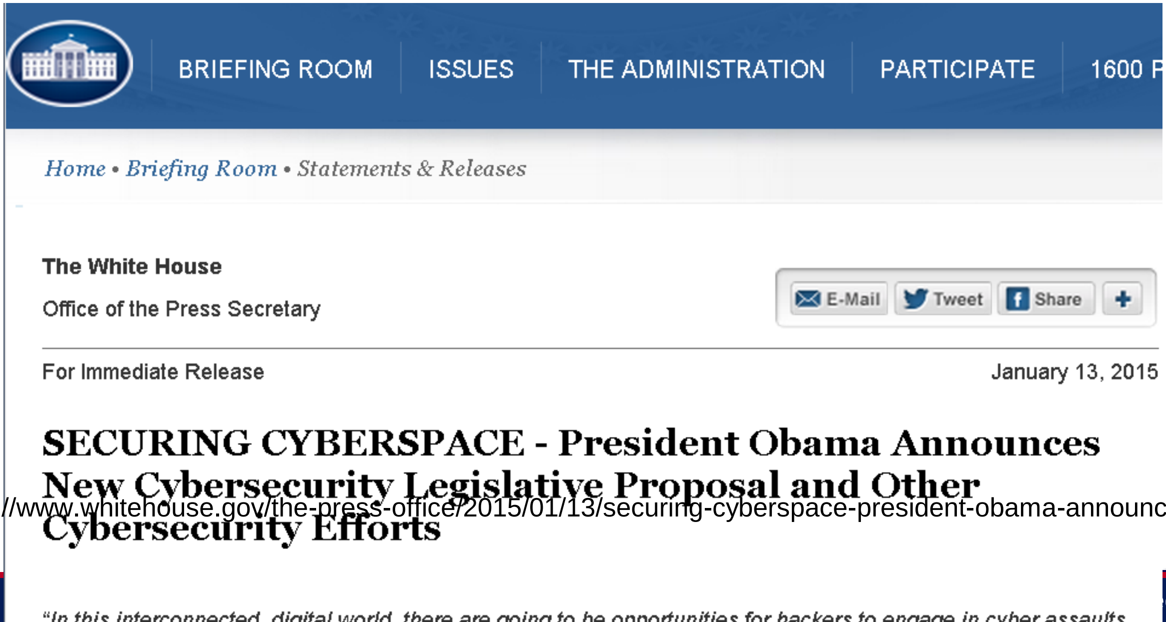
- Manpower:
  - – Talent isn’t cheap; it’s a seller’s market
  - – Government Accountability Office estimates a shortfall of 40,000 cyber security operatives
  - – Unlikely you will be able to get best of all skills:
    - If you do get a rock star, how will you keep him or her?
- Need to look outside:
  - – Service providers, consultants, other resources
  - – Leverage expertise of teams already assembled

Ref: http://thestack.com/us-army-gchq-cyber-warriors-needed-180215

Legislative Changes for 2015

Legislative changes for 2015

- President proposed new cyber-related legislation in State of the Union address on Jan. 20, 2015
- Six bills now before Congress
- Four bills signed into law December 2014



Home • *Briefing Room* • *Statements & Releases*

The White House

Office of the Press Secretary

For Immediate Release January 13, 2015

SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts

"In this interconnected, digital world, there are going to be opportunities for hackers to engage in cyber assaults

Ref: https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat

What Hath Congress Wrought?

- Cybersecurity bills before Congress in 2015
  - H.R.1731 - National Cybersecurity Protection Advancement Act of 2015
    - Passed House vote 355-63 on 23 April 2015
  - H.R.1560 - Protecting Cyber Networks Act
    - Passed House vote 307-116 on 22 April 2015; sent to Senate 27 April 2015
  - S.754 - Cybersecurity Information Sharing Act of 2015
  - S.456 - Cyber Threat Sharing Act of 2015
  - S.1241 - Enhanced Grid Security Act of 2015
  - S.1158 - Consumer Privacy Protection Act of 2015
- Four cybersecurity bills passed in December:
  - National Cybersecurity Protection Act of 2014 (now P.L. 113-282)
  - Federal Information Security Modernization Act 2014 (now P.L. 113-283)
  - Border Patrol Agent Pay Reform Act of 2014 (now P.L. 113-277)
  - Cybersecurity Workforce Assessment Act (now P.L. 113-246)

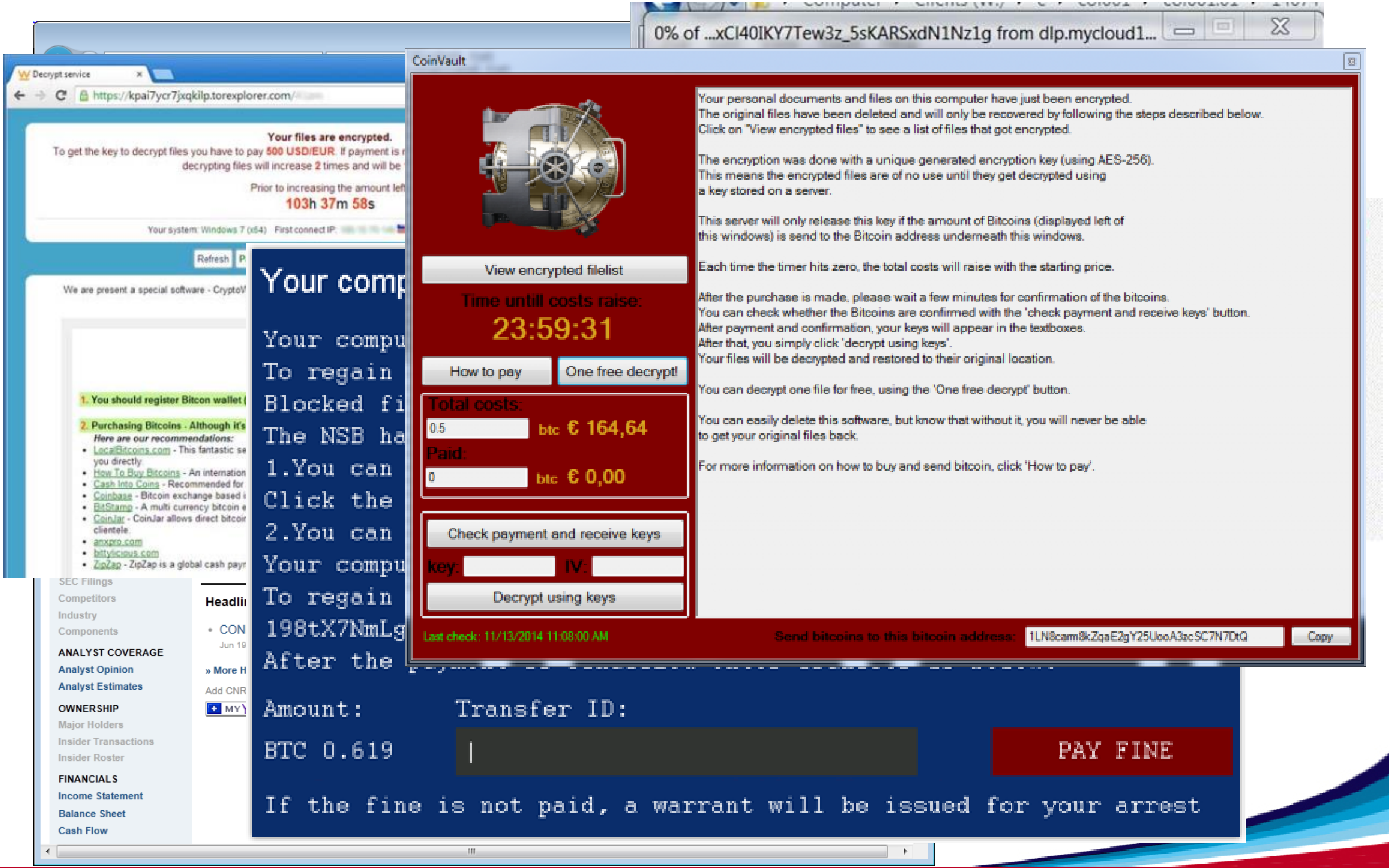
Ref: https://www.congress.gov

Attacking the Human

Attacking the Human in the Loop

- Common element in nearly every large-scale attack is a successful phishing event:
  - Visit infected website
  - Open malware-laced attachment
  - Click on link that goes elsewhere
  - Find a "lost" USB drive and plug it in to see what's on it
- No technology can fully protect against user ignorance

Beware! Ransomware is There!



Your files are encrypted.

To get the key to decrypt files you have to pay **500 USD/EUR**. If payment is
decrypting files will increase **2** times and will be

Prior to increasing the amount lef
103h 37m 58s

Your system: Windows 7 (x64)   First connect IP:

We are present a special software - CryptoW

1. You should register Bitcon wallet (

2. Purchasing Bitcoins - Although it's

Here are our recommendations:

- LocalBitcoins.com - This fantastic se you directly
- How To Buy Bitcoins - An internation
- Cash Into Coins - Recommended for
- Coinbase - Bitcoin exchange based i
- BitStamp - A multi currency bitcoin e
- CoinJar - CoinJar allows direct bitcoir clientele
- anxpro.com
- bittylicious.com
- ZipZap - ZipZap is a global cash payn

Your comp

Your compu
To regain
Blocked fi
The NSB ha
1.You can
Click the
2.You can
Your compu
To regain
198tX7NmLg
After the

Amount: BTC 0.619

Transfer ID:

If the fine is not paid, a warrant will be issued for your arrest

Time untill costs raise:
23:59:31

Total costs:
0.5 btc € 164,64

Paid:
0 btc € 0,00

Your personal documents and files on this computer have just been encrypted.
The original files have been deleted and will only be recovered by following the steps described below.
Click on "View encrypted files" to see a list of files that got encrypted.

The encryption was done with a unique generated encryption key (using AES-256).
This means the encrypted files are of no use until they get decrypted using
a key stored on a server.

This server will only release this key if the amount of Bitcoins (displayed left of
this windows) is send to the Bitcoin address underneath this windows.

Each time the timer hits zero, the total costs will raise with the starting price.

After the purchase is made, please wait a few minutes for confirmation of the bitcoins.
You can check whether the Bitcoins are confirmed with the 'check payment and receive keys' button.
After payment and confirmation, your keys will appear in the textboxes.
After that, you simply click 'decrypt using keys'.
Your files will be decrypted and restored to their original location.

You can decrypt one file for free, using the 'One free decrypt' button.

You can easily delete this software, but know that without it, you will never be able
to get your original files back.

For more information on how to buy and send bitcoin, click 'How to pay'.

Last check: 11/13/2014 11:08:00 AM

Send bitcoins to this bitcoin address: 1LN8carm8kZqaE2gY25UooA3zcSC7N7DtQ

Ref: KnowBe4.com

The Race for More Payment Card Info

- Visa and MasterCard have changed liability equation for card fraud:
  - New rules started on Oct. 1, 2015
- Already seeing large-scale harvesting
  - Target, Sally, PF Chang, Michaels, Home Depot …
- Common element: Memory-scraping malware
  - How did it get in?
  - How long was it there before detected?
  - How did it get the information out of the network?

Managing Risk in a Brave New World

Security Is All About Managing Risk

- We must manage RISK
  - Risk = Threat x Vulnerability x Asset Value
- Goal: Manage risk by reducing exposure
- We do so with CONTROLS
  - Technical controls: Affects computer systems
    - Implement with software or hardware
  - Administrative controls: Affects people and organization
    - Implement with policy and procedures
  - Physical controls: Affects environment and devices
    - Implement with equipment and add-ons

Risk Flavors

- Financial risk
  - What will it cost the bottom line if attack succeeds?
- Reputational risk
  - Will we lose customers or be unable to attract new ones?
- Legal risk
  - Will we get fined or even have an executive go to jail?
- Regulatory risk
  - Will we lose our charter to operate? (e.g., bank)

Leveraging Expertise

Fielding Security Force Cost Prohibitive

- JPMorgan cyber $500M in ‘15
  - Doubled last year spending
- Target breach costs and remediation could exceed $1B
- White House $13.9B budget for FY 2016
- Department of Homeland Security budget request $3.1B for FY 2016 for NPPD
- If you have security budgets like this…
  - Hire ME!

Ref: http://www.wsj.com/articles/j-p-morgan-to-accelerate-timeline-for-cybersecurity-spending-boost-1438641746
http://www.infosecurity-magazine.com/news/target-breach-costs-could-total-1bn/
http://federalnewsradio.com/budget/2015/04/dhs-defends-fy-2016-cyber-budget-before-senate-subcommittee/
http://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf

You Need Leverage

- Banks use leverage to complete purchases
- You use leverage to buy a home
- Leverage the expertise of trusted third-party for security:
  - Economical solution to risk management while
  - Reducing security vulnerabilities in the enterprise
- Things are changing too fast:
  - "Half of what you know about security will be obsolete in 18 months."*

* - G. Mark's corollary to Moore's Law

Where Do We Go From Here?

Next Steps

- Accept that we can’t go back to a simpler time
- Understand your enemy as much as possible
- Develop a battle plan for before, during, and after attacks
- Synthesize intelligence to stay informed
- Leverage security resources from trusted partners
- Take action decisively
- Stay ahead of the game

Cyber Leadership:

How to Win the Battle AND the War

G. Mark Hardy, CISSP, CISM, CISA
gmhardy@nationalsecurity.com
+1 410.933.9333
@ g_mark

Clausewitz portrait public domain; ref: http://commons.wikimedia.org/wiki/File:Carl_von_Clausewitz.PNG
Unless noted otherwise, presentation images licensed from Shutterstock: http://www.shutterstock.com/licensing.mhtml