



*Cyber Threats to Private Equity*  
Association for Corporate Growth (ACG) Webcast  
December 10, 2014



# Agenda

Topic
Introduction
Security statistics
Threat overview
Hacker economics
Security threats to private equity
Recommendations
Summary

# Introduction

## Daimon Geopfert

- McGladrey National Leader, Security and Privacy Consulting
- Located in Detroit, MI
- I like standardized tests
  - GCIH, GREM, CEH, CISSP, CISA, CISM
- I am not an auditor, but I play one on your network
  - Penetration testing
  - Vulnerability assessment
  - Security monitoring
  - Incident response
  - Forensics and investigations
- Former DoD, AFOSI-CCI, AIA
- All business, all the time



# Security Statistics

# Security statistics

- Breaches detected in first 24 hours: 1%-2%
- Breaches with data loss in first 24 hours: 60%-68%
- Breaches detected by an external 3rd party: 71%-92%
- Breaches undetected for two years or more: >14%
- Average days discovery: 87-210
- Average total cost per breach: \$5,407,820
- Average insurance payouts: \$954,253 - \$3.5 million

Compiled from:

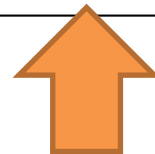
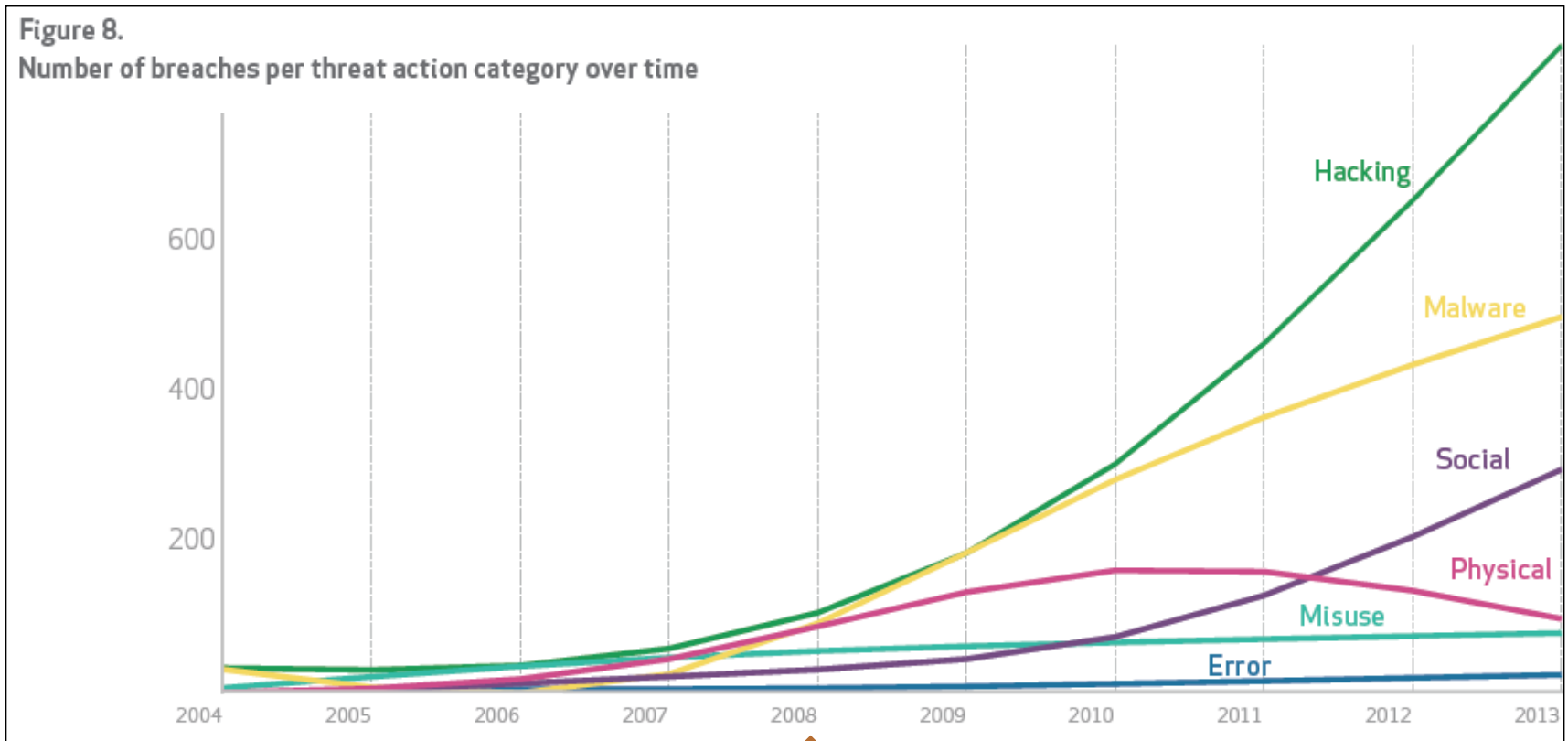
- Trustwave Global Security Reports
- Verizon Data Breach Investigations Reports
- Symantec Internet Security Threat Reports
- Cisco Annual Security Reports
- McGladrey internal studies
- Multiple other sources

# Security statistics

- To boil that down to plain English:
  - Clients are often incapable of knowing they've been breached in a reasonable timeline
  - The speed of the attackers versus the speed of the defense is highly in favor of the attackers
  - Most clients find out they've been breached from someone else which often leaves them blind about what to do
  - Breaches often run for extensive amounts of time
  - Client incident response plans are often built on the assumption that they'll detect the issue quickly, have significant knowledge of the issue, and can respond immediately
  - Breaches are expensive and getting more so, but insurance is becoming more restrictive and becoming more so (i.e., the worst of both worlds)

# Security statistics

## What are the methods?



2014 Verizon Data Breach Report

# Threat Overview



# Security threat – social engineering

- Fancy name for traditional “con games”
  - Attacking an environment via manipulating people
  - Focused on user habits, mannerisms, human nature, entrenched organizational procedures and activities
- Hacking by the KISS principle
  - Keep it simple, stupid
- Why go through all of the effort to bypass firewalls, anti-virus, monitoring solutions, etc.?
- Why not just have the target do all the work for you?

**SOCIAL ENGINEERING  
SPECIALIST**

Because there is no patch  
for human stupidity

# Security threat – social engineering

- Example KISS attack: credential harvesting

*Dear [Individual Name],*

*[Target] is committed to ensuring we provide a positive employment experience while pursuing a customer-focused business strategy. Therefore, we have contracted with an external survey company to randomly survey our employees to gauge how we are doing in this endeavor. Management has already been notified of this survey.*

*We understand that you are very busy, but please take a few minutes to access and complete the questionnaire. In order to access the questionnaire, you will first need to click on the following [link](#), this will take you to the survey specially prepared for [Target].*

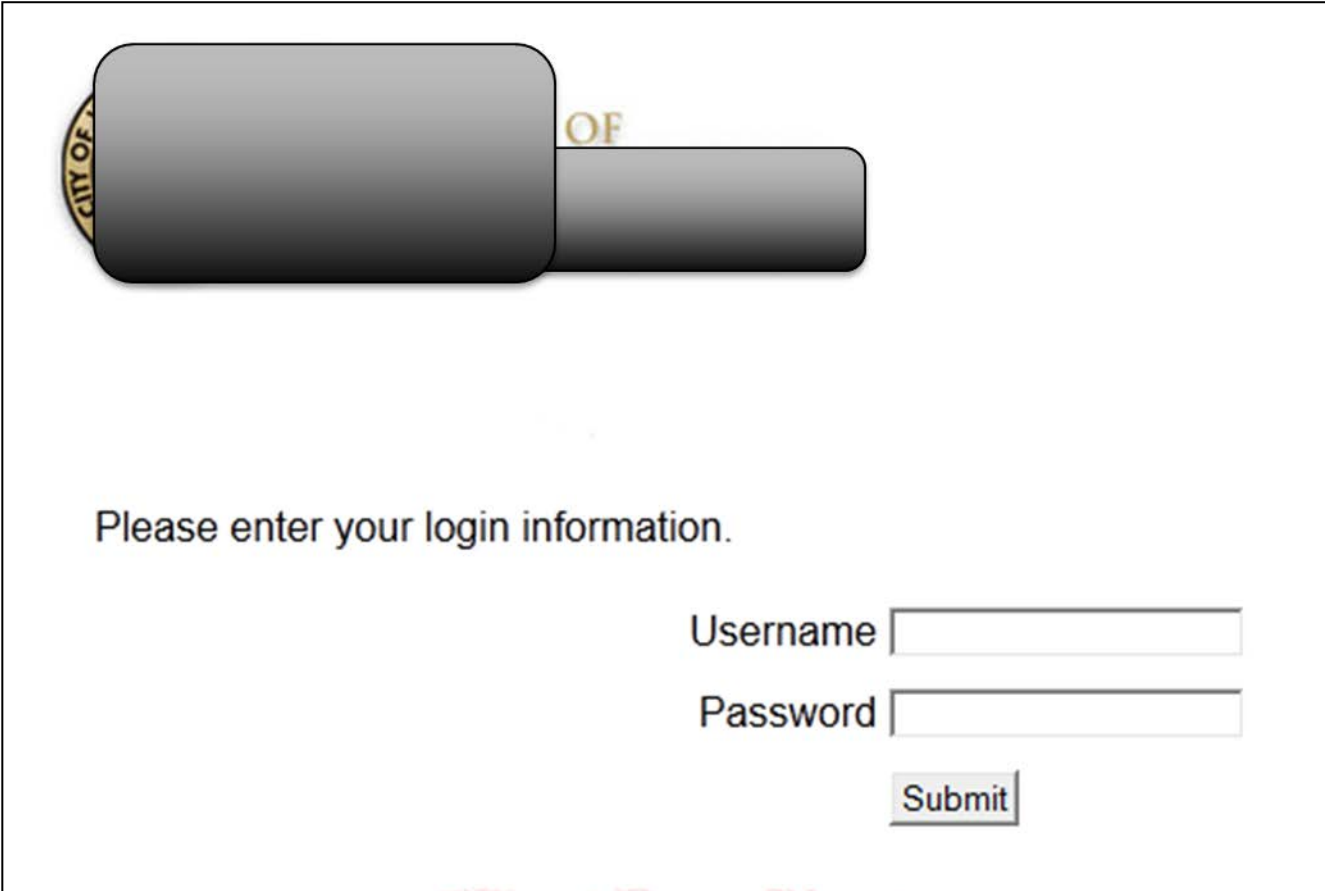
*Link: [http://ssl.\[temp\].com/survey](http://ssl.[temp].com/survey)*

*We appreciate your prompt attention to this matter. The results of the questionnaire will be emailed to all participants in three to four weeks. As an added bonus, 10 respondents will be randomly selected to win a new [iPad 4](#).*

*Thank You,  
[Target]  
Human Resources Department*

# Security threat – social engineering

- Example KISS attack: credential harvesting



The image shows a screenshot of a web page. At the top left, there is a logo for the City of [redacted] with the text "CITY OF" visible. The main content of the page is obscured by a large grey rectangular redaction box. Below the redaction, the text "Please enter your login information." is displayed. Underneath this text, there are two input fields: "Username" and "Password". Below the "Password" field is a "Submit" button. This setup is a classic example of a KISS (Keyboard Input Sniffing) attack, where the legitimate page content is replaced by a malicious form designed to harvest user credentials.

# Security threat – client-side attacks

- What is a client-side attack?
  - Flip the attack model on its head
  - Traditional attacks are “server-side”
  - The attacker goes after a service being “served” by the target
  - In plain English, the attacker is going to the target system and directly attacking some resource



Mr. Hacker



Ports:

80

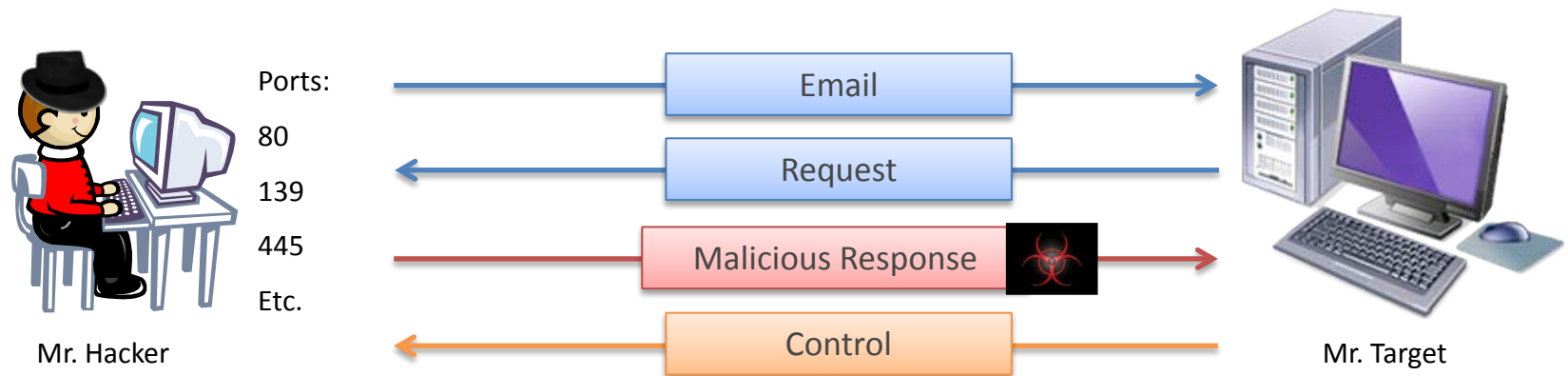
139

445

Etc.

# Security threat – client-side attacks

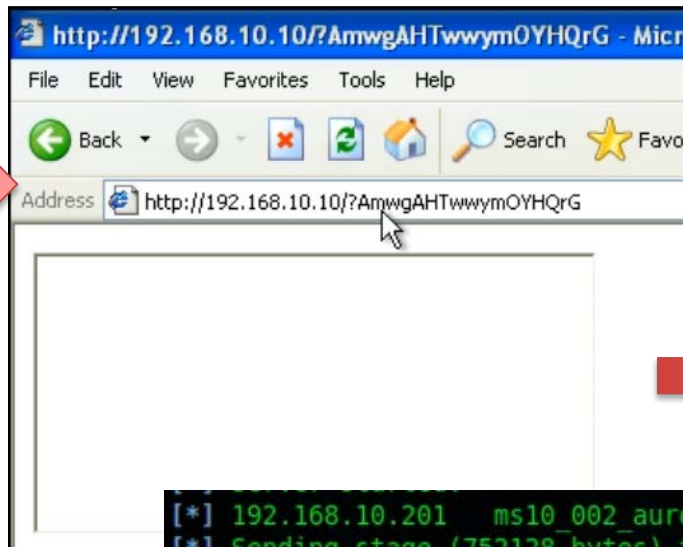
- A client-side attack means the attacker takes the role of the server and the victim is acting as the client
  - The attacker offers something to the target
  - In plain English, the attacker needs the target system to come to them or accept something from them
  - Can be as simple as viewing a web page but can also involve local files such as documents



# Security threat – client-side attacks

- Client-side attacks are effective because many organizations struggle patching non-OS software
- Web browsers, Java, Adobe, QuickTime, etc.

Name	Disclosure Date	Rank	Description
exploit/windows/browser/ms10_002_aurora	2010-01-14 00:00:00 UTC	normal	Internet Explorer "Aurora" Memory Corruption



```
[*] 192.168.10.201 ms10_002_aurora - Sending Internet Explorer "Aurora" Memory Corruption
[*] Sending stage (752128 bytes) to 192.168.10.201
[*] Meterpreter session 1 opened (192.168.10.10:55555 -> 192.168.10.201:1095) at 2012-08-17 1
```

# Security threat – custom malware

- Common controls
  - Is anti-virus deployed?
  - Is it on users systems, servers, mail, etc.?
  - Are the signatures updated regularly?
  - Are scans run regularly?
- Reality
  - Attackers purchase the same subscriptions and appliances as everyone else in order to perform QA of their malware products.
  - AV, being signature based, is limited to what it knows.
  - What happens if attackers make AV look different?
  - Many organizations are dealing with malware outbreaks of varying scales, on a monthly basis.

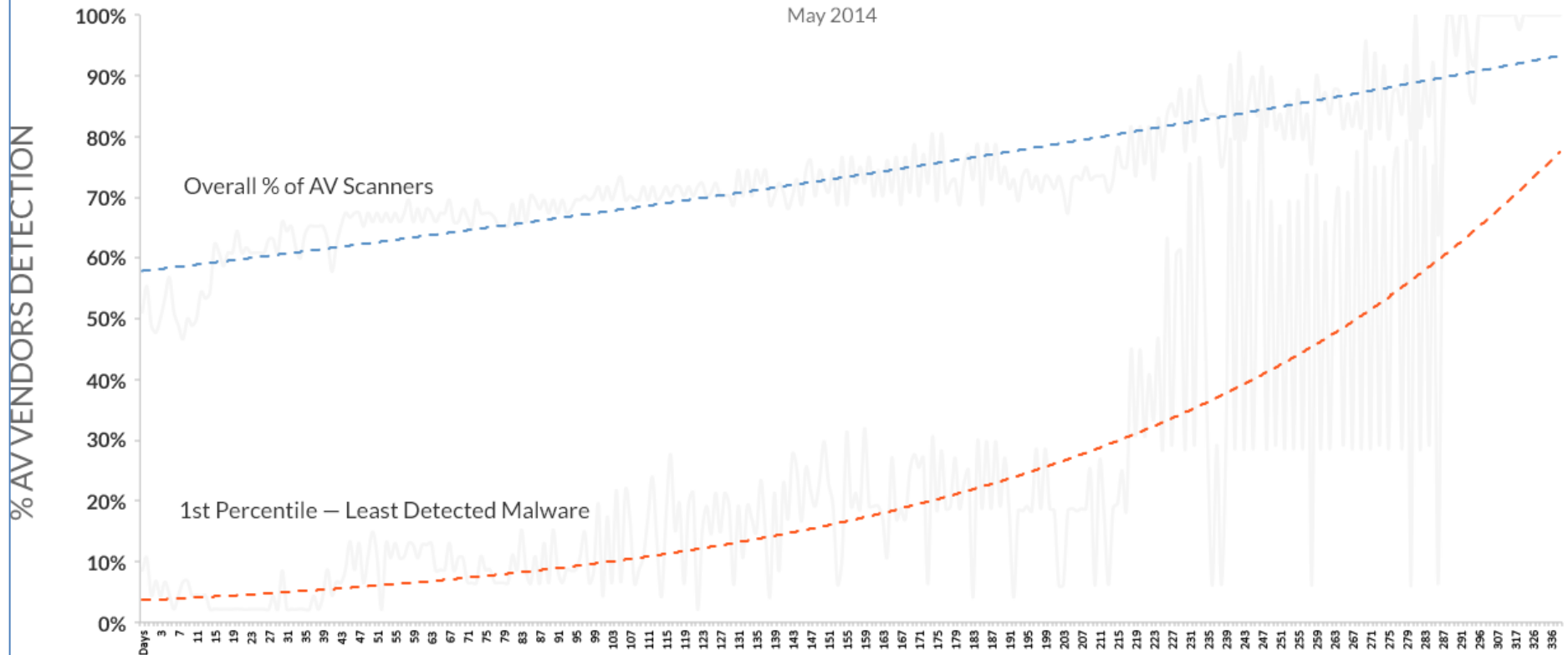


# Security threat – custom malware

INTERNET SECURITY THREAT REPORT

## Probability of Malware Detection for Antivirus Solutions

May 2014



Data collected and research performed by Lastline Labs. For more information, please visit [www.lastline.com/labs](http://www.lastline.com/labs).



# Hacker Economics

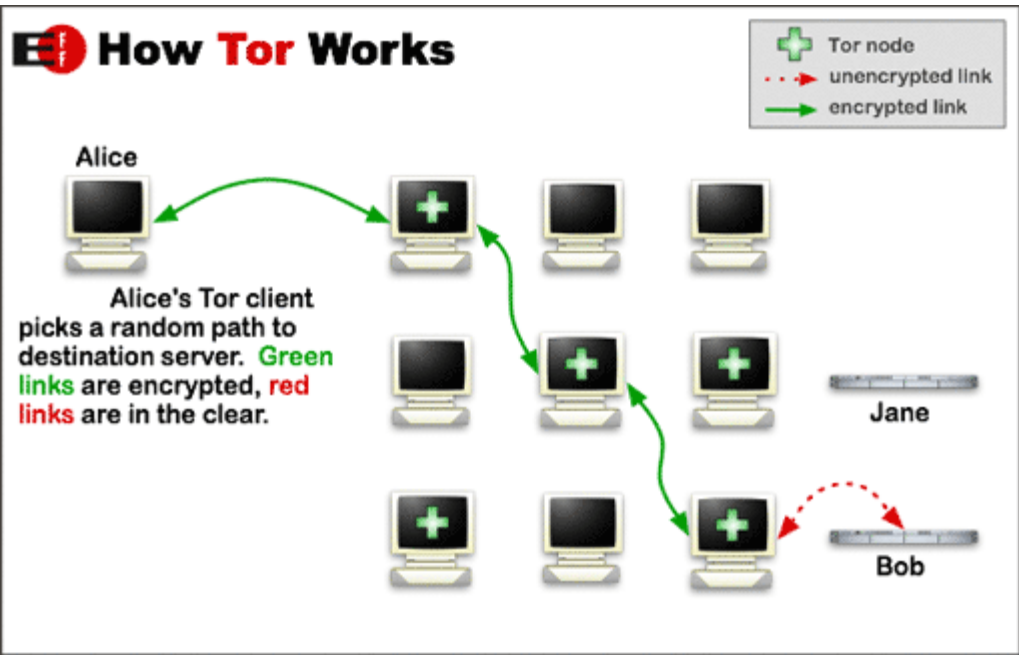


# Hacker economics

- Understand how they make money and you'll understand the attackers
- Targeted versus target of opportunity
- Anything that can be monetized
  - CC
  - PII
  - Bank accounts
  - Intellectual property
  - Bandwidth and systems
  - Medical data/PHI
- Bounties and auctions

# Hacker economics

## How Tor Works



The screenshot shows the Tor Browser Startpage. At the top, it says "Congratulations! This browser is configured to use Tor. You are now free to browse the Internet anonymously." Below this is a search bar with the text "Search securely with Startpage." There are two boxes: "What Next?" which says "Tor is NOT all you need to browse anonymously! You may need to change some of your browsing habits to ensure your identity stays safe." and "You Can Help!" which lists "Run a Tor Relay Node", "Volunteer Your Services", and "Make a Donation". At the bottom, it says "The Tor Project is a US 501(c)(3) non-profit dedicated to the research, development, and education of online anonymity and privacy. Learn more about The Tor Project »".

# Hacker economics

Subscribe Now

## Official Marketpla

Marketplace Comparison Chart  
*Referral links can be found in the market's specific subreddit.*  
**Do NOT post them here!**

---

### Multisig Escrow Markets

**Alpaca Marketplace:**  
alpaca7bcqv2rnu3.onion

**BlackBank / BB:**  
wztyb7v1fcw6l4xd.onion

**Cannabis Road / CR:**  
cannabiskofv17pa.onion

**Cloud-Nine / C9:**  
bviaqyj6obc54vhn.onion

**Evolution / Evo:**  
k5zq47j6wd3wdvjg.onion

**Hydra:**  
hydrampvvnunild1.onion

**The Marketplace (TMP):**  
Tor: 43y5mwjvhxd6zf7v.onion  
i2p: themarketplace.i2p

**The Pirate Market:**  
yjhzeed15osagmmr.onion

**TOM Marketplace:**  
tom3j5jkj17327oc.onion

**Tor Bazaar / TB:**  
bazaarlv2a7i3uyn.onion

1776 Marketplace; WARNING  
n6tznxy7sod7eqt.onion

Subscribe Now

## Centralized Escrow Markets

**Agora:**  
agorahooawayyfoe.onion

**Andromeda:**  
andromedam363aux.onion

**BlueSky / BSM:**  
blueskyplzv4fst1.onion

**Middle Earth Marketplace (requires Javascript):**  
mango7u3rivtwxy7.onion

**Outlaw Market:**  
outfor6jwcztwbpd.onion

**The Majestic Garden / TMG:**  
themgpeuawtfvz1.onion

**Torbook (requires Javascript):**  
torbookdjwhjnju4.onion

**Underground Marketplace:**  
unground6baopdio.onion

**Pandora; WARNING:**  
pandorajodqp5zrr.onion

Silk Road 2 / SR2; WARNING:  
silkroad6ownowfk.onion

---

### Bitcoin Tumbling Services:

**Bitcoin Fog:**  
fogcore5n3ov3tui.onion

**BitBlender:**  
bitblendervrfkzr.onion

**Helix, By Grams:**  
gramsflow.com/helix

BlackBank ₿
founded on January 7, 2014  
19057 members

## Market

http://wztyb7v1fcw6l4xd.onion

Transactions

**Transaction Fees**  
Deposits: Free

*User-to-User*  
USD: \$0.01 + 3.0 % USD  
BTC: 0.00001964 + 3.0 % BTC

*Withdrawal*  
BTC: 0.0001 + 0.1 % BTC

Exchange Rates

USD \$509.28 USD/BTC  
 GBP £325.24 GBP/BTC  
 EUR €389.08 EUR/BTC  
 AUD A\$597.07 AUD/BTC

BTC rates are based on the average of all exchanges and sourced from:  
<https://bitcoinaverage.com>

Server Time: 2014-08-14 12:18:09

## Welcome to BlackBank

### Features

- All Bitcoin transactions are automatic, the system with funds being available
- Fully optional automated and easy to use, funds are deposited to vendor's address as soon as possible immediately after accepting a purchase
- Auto-Finalize releases funds to vendor** auto-finalize period can be extended
- Fully integrated messaging and order management are handled in a timely manner.
- Free Vendor Account for vendor**
- Straight forward inventory and sales
- Manage ship-to locations, individual
- Save the ship-to locations in a list as well as shipping fees one-by-one

# Hacker economics

$$510\text{USD} * .0135\text{BTC} = \$6.89$$

The screenshot shows a browser window with the URL `k5zq47j6wd3wdvjg.onion/listing/12538`. The page header includes a user profile for 'qwerty987' with a balance of 'BTC 0.0000'. The marketplace logo 'evolution' and a search bar are visible. The listing is for 'CC from the US (Centurion, Signature & Platinum)' by user 'railguycc' (99.2% rating, Level 4 with 664 reviews). The price is listed as 'BTC 0.0135'. The item is 'In stock' and has a 'Buy It Now' button. A quantity selector is set to '1'. Below the main listing, there are tabs for 'Details', 'Feedback', and 'Return Policy'. The 'Description' tab is active, showing a list of provided details and a disclaimer about CVV replacement.

[Details](#) [Feedback](#) [Return Policy](#)

### Description

Fresh and valid! That's what I like! Cust. Support included!

I only send out Centurions, Signatures & Platinums!

Details that are provided;

- CCnumber / exp. date / sec. code
- Full name
- Full address including ZIP
- (Phonenumber) not always
- (Emailaddress) not always

Cards will be replaced when dead, but please let me now in 60 minutes after you received your info.  
\* CVV will not be replaced cause of low balance  
\* CVV will only be replaced when my private checkers tells me that the CVV is invalid.  
\* CVV will not be replaced when you are to late letting me know your opinion that cc is not working.

When you don't agree these point, please don't order.

### Ships To

Worldwide

# Hacker economics

The screenshot shows a marketplace listing for American Express cards. The user is logged in as 'qwerty987' and has a balance of 'BTC 0.0000'. The listing is by 'eXe\_eXe' (Level 4, 498 items). The price is 'BTC 0.0000' and it is 'In stock'. The quantity is set to 1. The 'Option' dropdown menu is open, showing several choices with their respective BTC prices: 2 CVVs (RANDOM) -- 1 day (+ BTC 0.0329), 5 CVVs (RANDOM) -- 1 day (+ BTC 0.0677), 10 CVVs (RANDOM) -- 1 day (+ BTC 0.1354), 20 CVVs (RANDOM) -- 1 day (+ BTC 0.2516), 50 CVVs (RANDOM) -- 1 day (+ BTC 0.5032), 1 CVV NON-VBV (out of stock) -- 1 day (+ BTC 10.0000), and 1 Fulls -- 1 day (+ BTC 0.0483). The 'Buy It Now' button is highlighted in red. Below the listing, there are tabs for 'Details', 'Feedback', and 'Return Policy', and a 'Report listing' link. The 'Description' section contains a string of stars, a link to a listing, and information about American Express cards.

Welcome back, **qwerty987**    📧 0    📧 0    🛒 0    💰 BTC 0.0000    🏠 Home    👤 My Evolution    🚪 Logout

**evolution**    Search products, vendors, ...    🔍 Search

**instant delivery**  
By **eXe\_eXe** ( 100.0% )    **Level 4 ( 498 )**

**BTC 0.0000**  
In stock.

Qty: 1

**Buy It Now**

**Option**

- 2 CVVs (RANDOM) -- 1 day ( + BTC 0.0329 )
- 5 CVVs (RANDOM) -- 1 day ( + BTC 0.0677 )
- 10 CVVs (RANDOM) -- 1 day ( + BTC 0.1354 )
- 20 CVVs (RANDOM) -- 1 day ( + BTC 0.2516 )
- 50 CVVs (RANDOM) -- 1 day ( + BTC 0.5032 )
- 1 CVV NON-VBV (out of stock) -- 1 day ( + BTC 10.0000 )
- 1 Fulls -- 1 day ( + BTC 0.0483 )

Details    Feedback    Return Policy    Report listing

**Description**  
NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★NEWS★  
IF YOU HAVE FAVOURITE BINS BUY FROM THIS LISTING:  
<http://k5zq47j6wd3wdvjq.onion/listing/21379>

LISTING★LISTING★LISTING★LISTING★LISTING  
American Express High Validy cards and Very Fresh. Centurion/Platinum.  
Visa/Mastercard  
all cards are checked and random, all fresh and high validy.

$$510\text{USD} * .5032\text{BTC} = \$256.63$$

$$256.63\text{USD} / 50 = \$5.13$$

# Specific Threats to Private Equity

# Threats to private equity

- What happens if you own or acquire a company not knowing that it has suffered a data breach and will be facing fines, litigation, and increased oversight?
- What happens if a potential target has been making itself more attractive by deferring maintenance and upgrade costs?
- What happens if a target with a large footprint of sensitive data is not overly accurate in documenting where that data is, who has access to it, and how it is protected?



# Threats to private equity

- Competitive intelligence
  - Very pretty name for very ugly business methods.
  - How much do you think a \$12 billion hedge fund would pay to have a peek at your acquisition plans if you're going to take a public company private? The quarterly financials for a publicly traded company the day before they hit the street?
- What happens if you divest a company and sign assurances that it is secure and compliant? (and it isn't...)
- What happens if you own or acquire a company not knowing its key intellectual property has been compromised?

# Threats to private equity

## DealB%k

### Cyberattacks a Huge Threat to Start-Ups, and Their Investors

By CRAIG A. NEWMAN AND DANIEL L. STEIN

- Intellectual property showing up on the streets of Shanghai before it shows up in U.S. markets.
- Private equity and angel investors often blind to this new risk and how it impacts their investments.
- Because of the focus on the bottom line, expenses related to data protection are of then the first sacrifice.
- Studies show good protection can save ~\$1 million per year, high-end protection can save ~\$2 million per year.



Trion

A report said a Chinese hacking ring infiltrated the servers of dozens of video gaming companies, including Trion Worlds, which publishes Defiance.

# Threats to private equity

- SEC OCIE cyber security
- “Take-home test” for any financial institution or regulated firm preparing for OCIE examination or conducting internal audit.
- Well, doesn’t that sound benign.
  - Take-home test. Information gathering. Partnership opportunities.
- However ,many elements of the risk alert mirror elements of not-so-benign regulatory obligations.
  - Section 30 of Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information (17 CFR §248.30)
  - Securities Exchange Act Rule 15c3-5: Risk Management Controls
  - Identity Theft Red Flag Rules
  - Suspicious activity reporting requirements
  - Requirement relating to reasonable policies and procedures
  - State and federal data breach laws
- What if a weakness is exposed by the cyber security review?

# Threats to private equity

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MINNESOTA

ROBERT KULLA, Derivatively on  
Behalf of TARGET CORPORATION,  
  
Plaintiff,  
  
v.  
  
GREGG W. STEINHAFEL, BETH M.  
JACOB, JAMES A. JOHNSON,  
SOLOMON D. TRUJILLO, ANNE M.  
MULCAHY, ROXANNE S. AUSTIN,  
CALVIN DARDEN, MARY E.  
MINNICK, DERICA W. RICE, JOHN  
G. STUMPF, DOUGLAS M. BAKER,  
JR., HENRIQUE DE CASTRO, and  
KENNETH L. SALAZAR,  
  
Defendants,  
  
-and-  
  
TARGET CORPORATION, a  
Minnesota corporation,  
  
Nominal Defendant.

Case No. \_\_\_\_\_

**VERIFIED SHAREHOLDER  
DERIVATIVE COMPLAINT FOR  
BREACH OF FIDUCIARY DUTY  
AND WASTE OF CORPORATE  
ASSETS**

DEMAND FOR JURY TRIAL

Directors sit on the board of a portfolio

Company following the Target D&O

Directors and officers named in shareholder

## Directors Hit with Derivative

### NATURE OF THE ACTION

1. This is a verified shareholder derivative action by plaintiff on behalf of

nominal defendant Target Corporation

officers and members of

remedy defendants' violation

assets that have caused substantial

Plaintiff Maureen Collier ("Plaintiff"), by and through her attorneys, derivatively on behalf of nominal defendant Target Corporation ("Target" or the "Company"), submits this

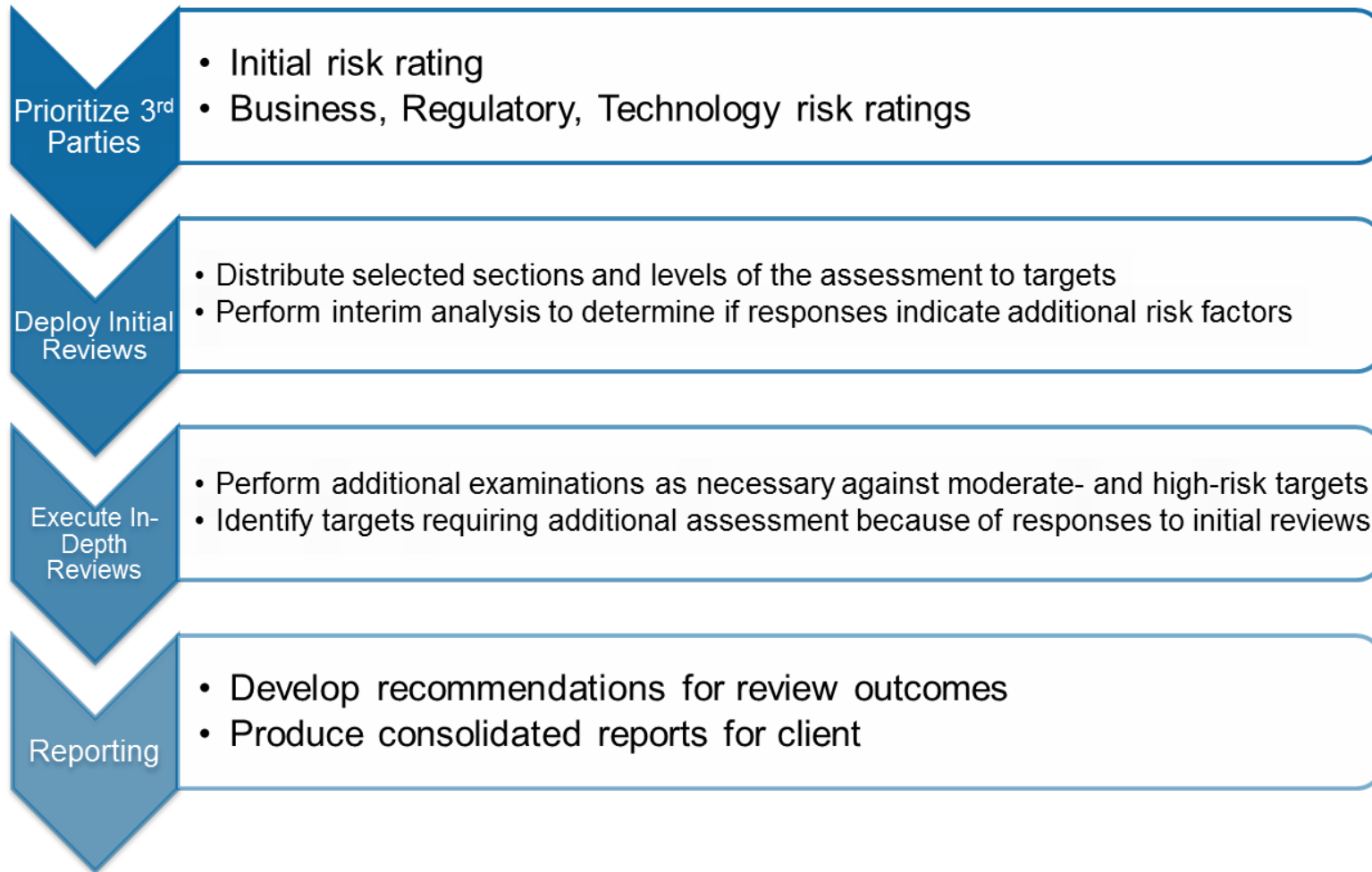
Verified Shareholder Derivative Complaint against the directors and officers named herein (collectively, the "Individual Defendants"). Plaintiff's allegations are based upon personal

# Recommendations

# Recommendations – Acquisition and management process

- What is it about the target that makes it of value to you?
- Is it something that can be stolen or copied? Broken?
- How would you know if it has been before you buy that target?
- How would you know if it has happened since you bought it?
- How are you monitoring this risk?
  - Are your targets or portfolio companies doing this on their own?
  - What evidence or metrics are provided to you?
  - Do you have some centralized process for keeping an eye on it?
- Is the target in an industry that is facing potential new regulatory oversight?
- What if the target isn't but its primary partners, customers, etc. are?
  - E.g., many retailers and financial clients are now forced to do extensive risk assessments on their vendors and partners
  - Are you prepared to deal with the cost of these?

# Recommendations – Acquisition and management process



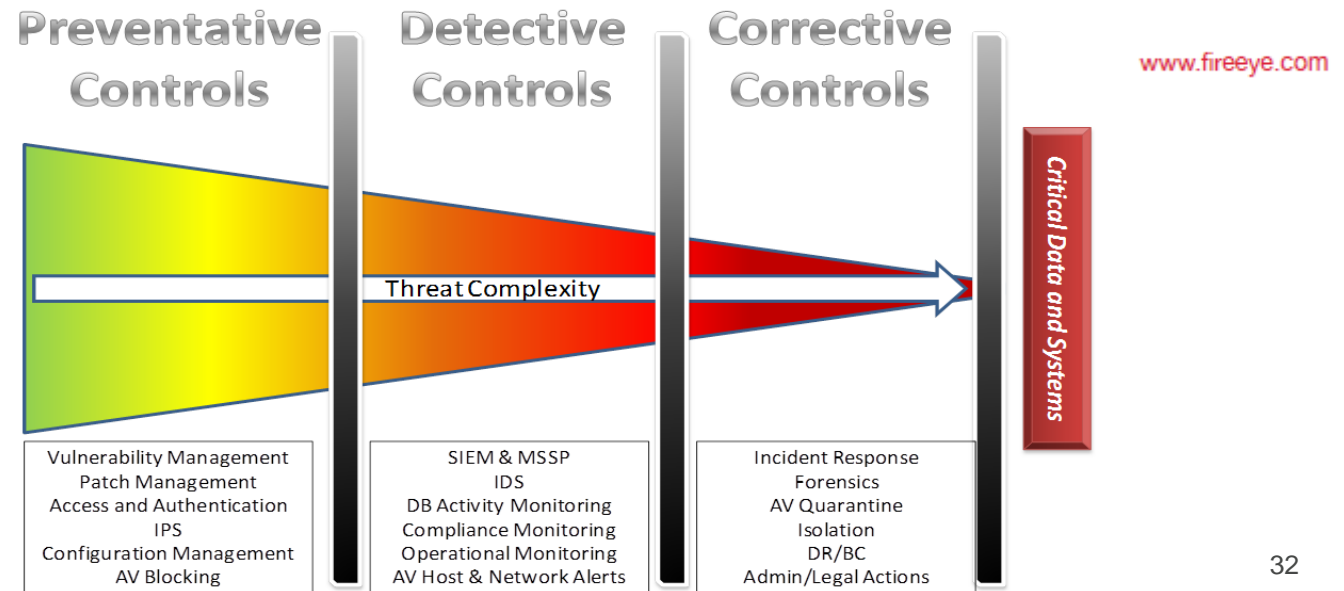
# Recommendations – Security posture

- Develop consistent, common security policies for use in portfolio companies
- AND/OR Require portfolio companies to map against a common standard such as ISO 27002, NIST sp800-53, etc.
- These help track if your program is complete
  - Less likely to get breached, more likely to notice they are breached, and respond effectively
- Litigation and insurance
  - Makes it hard to get sued or turned down for insurance claim
  - Air gaps = “auto fail” for lawsuits, fines, insurance
- Focus on long-term management
  - Metrics: You can’t manage what you can’t measure



# Recommendations – Monitoring

- How do you know portfolio companies are keeping up with security after initial reviews?
- Are they capable of know if they have been breached?
- Slow speed of detection compounds all other costs
- If you can detect an attacker early enough in the breach you can remove them before damage is done



# Recommendations – Incident response plan

- This is more than having a plan, it is having the supporting components to make it work.
- The costs of consultants skyrockets when we have to work in an environment that was not ready to do IR.
  - No logs, wrong architecture for emergency monitoring, failed initial response damaging evidence, no baseline to identify anomalies, lack of asset and configuration management, lack of data awareness.
  - Where is your stuff? Don't know. Who has access to it? Everyone.
- Recognize when you are in over your head.
  - The urge to try to manage it yourself is overwhelming.
  - Appearance of delaying can cost you later in lawsuits and fines.
  - “Please stop playing in my crime scene...”

# Recommendations – Third parties

- Portfolio companies and targets are moving large portions of their environment, processes, and data to third parties.
- How much control do they have over these third parties?
- What type of data do they maintain?
- What is in the contracts regarding data protection?
  - How is it validated?
- What is in the contracts regarding response and investigation?
  - If you take anything away from this point, this is it.
- Do you think the public will delineate between you being breached and your vendor being breached?
- You can outsource functionality but not responsibility.

# Recommendations – Insurance

- Policies can cover hazards which can cause security and privacy losses:
  - Virus and malicious code
  - Denial of service attacks
  - Hacker attacks and unauthorized access
  - Malicious hardware
  - Physical theft of device and media
  - Accidental release
  - Rouge employees
  - Social engineering
- Be aware of the changing nature of this insurance
  - Risk assessments used to set your premiums
  - Assessments after you file a claim to determine percentage of fault
  - Organization members facing individual lawsuits

# Summary

# Summary



- Don't panic
- Plan to fail, but plan to fail gracefully
  - Ability to know when a control has failed
  - Ability to recover quickly and with minimal damage
  - Ability to handle administrative requirements of response
  - Consolidated, robust controls in a defense-in-depth manner are effective
- Just because the attacker got into the network doesn't mean they have won; the party just started
- Do not become a "hacker snack"
  - Hard and crunchy on the outside, soft and gooey in the middle
  - Every hoop you force the attacker to jump through is a chance for you to detect them... if you are watching
- You don't need to outrun the bear...

# Questions?

[daimon.geopfert@mcgladrey.com](mailto:daimon.geopfert@mcgladrey.com)