# THE POWER OF BEING UNDERSTOOD

AUDIT I TAX I CONSULTING

RSM

# BBNC ANNUAL COMPLIANCE CONFERENCE

## Cyber Security Autopsy

November 13, 2016

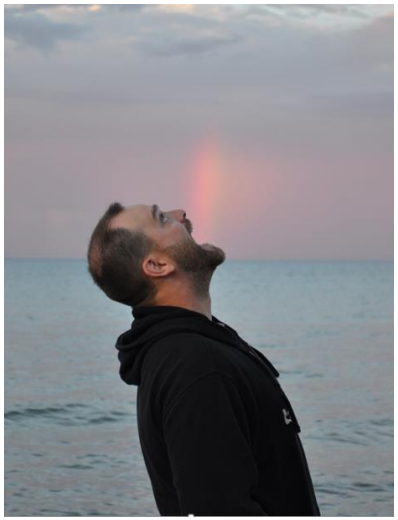
# Agenda

- Introduction
- Security Statistics
- Through The Mirror
- Recommendations

*90 Minutes

# Introduction

- Daimon Geopfert, RSM
  - National Leader, Security and Privacy Services
  - Located in Detroit, MI
  - I am not an auditor but I play one on your network
    - Penetration Testing
    - Vulnerability Assessment
    - Security Monitoring
    - Incident Response
    - Forensics & Investigations
  - Former DoD, AFOSI-CCI, AIA
  - I like standardized tests
    - GCIH, GREM, CEH, CISSP, CISA, CISM



# SECURITY STATISTICS

# Security Statistics
## Quick Hits

Compiled from:
- NetDiligence/RSM 2016 Annual Cyber Claims Study

## KEY FINDINGS

Breaches are not just for the Fortune 500 companies anymore.

The majority (87%) of claims submitted for this study are for organizations with revenues less than $2B.

The numbers of records lost can be large, no matter how large or small an organization may be.

Our dataset contains breaches of 1M or more records occurring in organizations of all sizes, except Mega Revenue (>$100B).

Breaches can be very costly, no matter how large or small an organization may be.

In our dataset, breaches with total costs greater than $5M occurred in organizations of all sizes except Mid Rev ($2–10B).

Breaches with few records can be very costly. One event in our dataset involved 1 record (PHI) with a cost of between $1.5–2.0M.

The average number of records lost was 2.04 million. The median number of records lost was 1,339.

The greatest numbers of exposed records occurred in the Financial Services (78M records) sector, followed by Retail (56M records).

# Security Statistics
## Quick Hits

Compiled from:
- NetDiligence/RSM 2016 Annual Cyber Claims Study

The average per-record cost was $17K. The median per-record cost was $39.82. This extraordinarily high per record average has been driven by three large outliers: fewer than 10 records each, with per record costs between $35K and $1.6M.

PII was the most frequently exposed data (40% of claims), followed by PCI (27%) and PHI (15%).

Hackers were the most frequent cause of loss (23%), followed by Malware/Virus (21%). Following at third and fourth were Staff mistakes (9%) and Rogue employees (7%).

Healthcare was the sector most frequently breached (19%), followed by Professional Services (13%).[1]

The average cost for Crisis Services (forensics, notification, credit monitoring, legal guidance/Breach Coach® and miscellaneous other response costs) was $357K. The median cost for Crisis Services was $43K.

The average cost for legal defense was $130K. The median cost for legal defense was $16K.

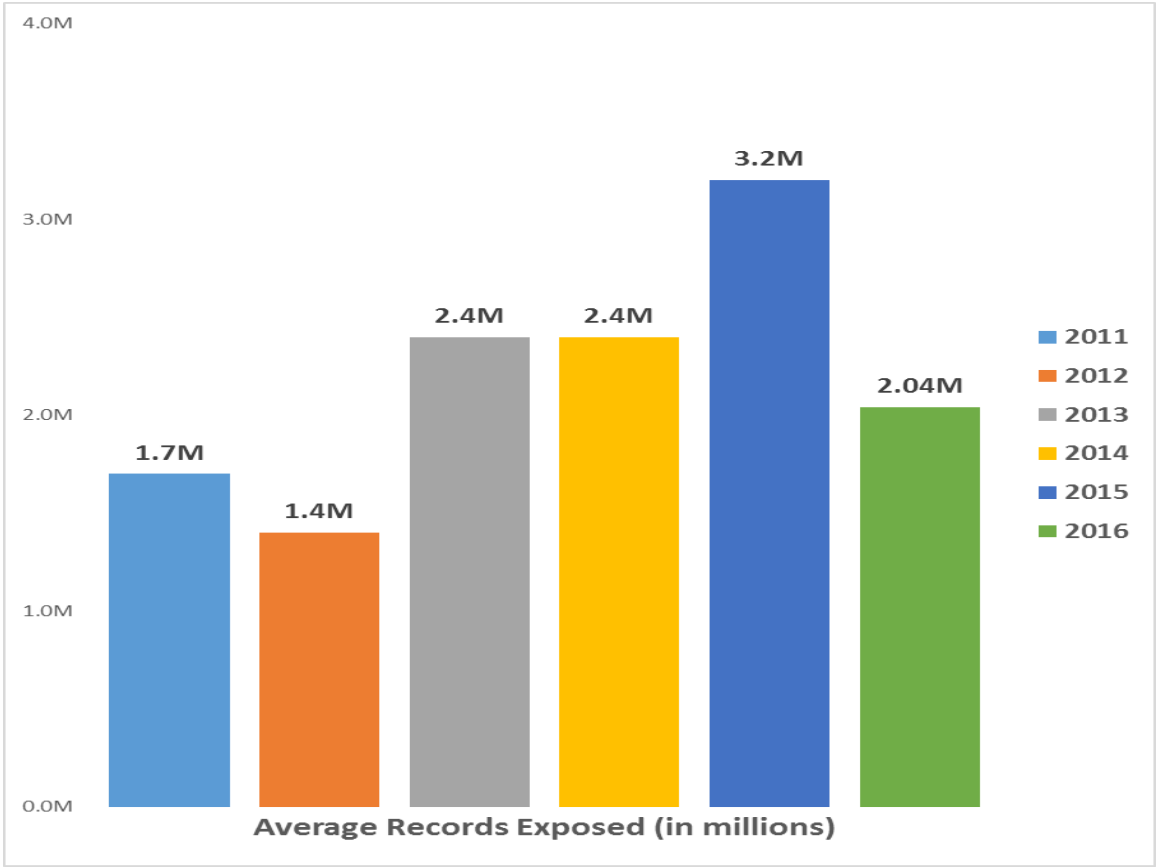
# Security Statistics
## Quick Hits

Compiled from:
- NetDiligence/RSM 2016 Annual Cyber Claims Study

- Third parties accounted for 13% of the claims.
- There was insider involvement in 30% of the claims.
  - This includes mistakes and errors
  - Also includes rogue employees and purposeful malicious actions
- The average cost for legal settlement was $815k.
- 75% of costs were tied to Crisis Services
  - Incident Response, hotlines, notifications, etc.
  - The costs were compounded by the organizations not having robust incident response plans
- Ransomware average costs were $32k but raising quickly
- The average claim payout was $495K.

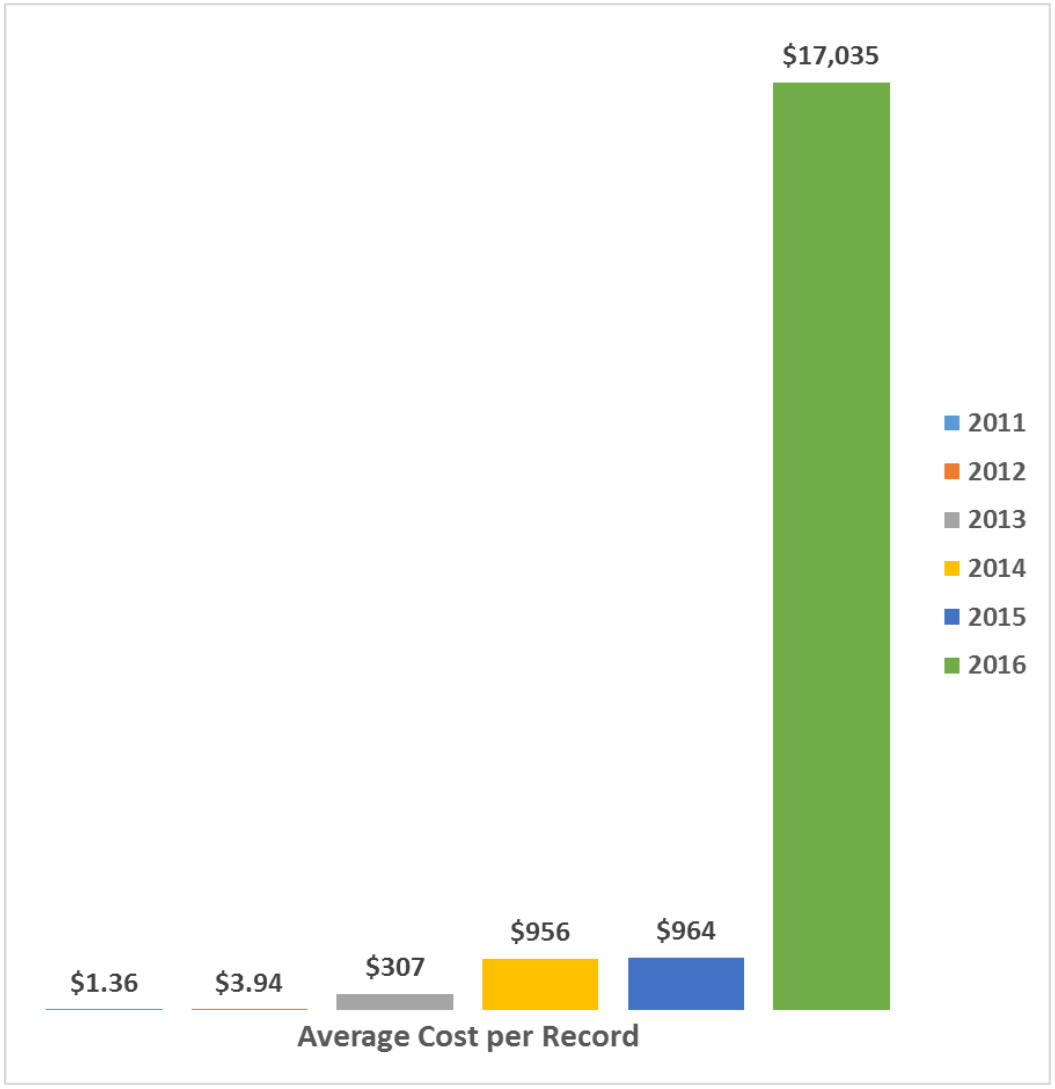
# Security Statistics

Compiled from:
- NetDiligence/RSM 2016 Annual Cyber Claims Study




# Security Statistics

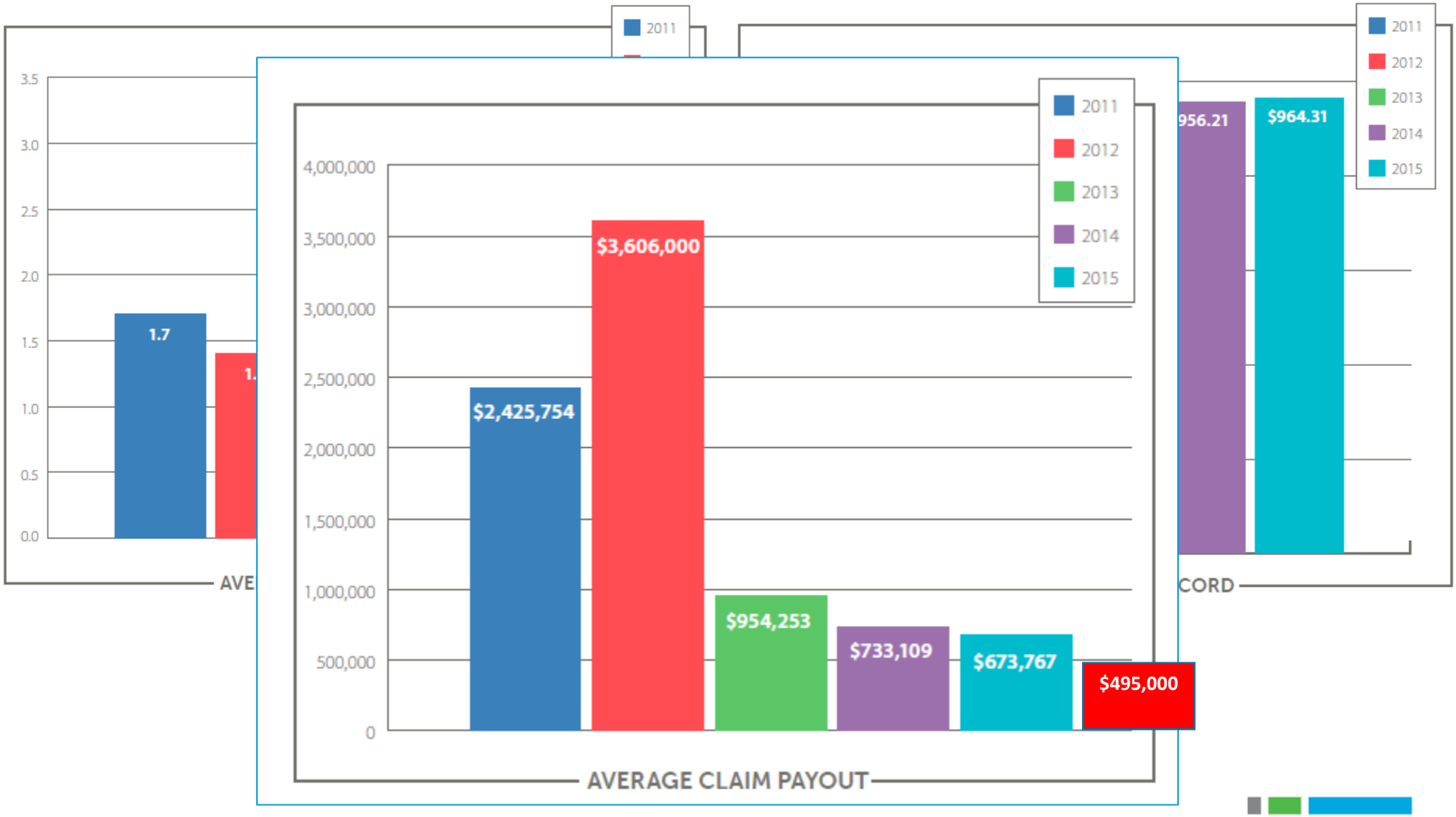
Compiled from:
- NetDiligence/RSM 2016 Annual Cyber Claims Study




# Security Statistics

## *Claims Payouts – Trend Continues*

Compiled from:
- NetDiligence/RSM 2015 & 2016 Annual Cyber Claims Study

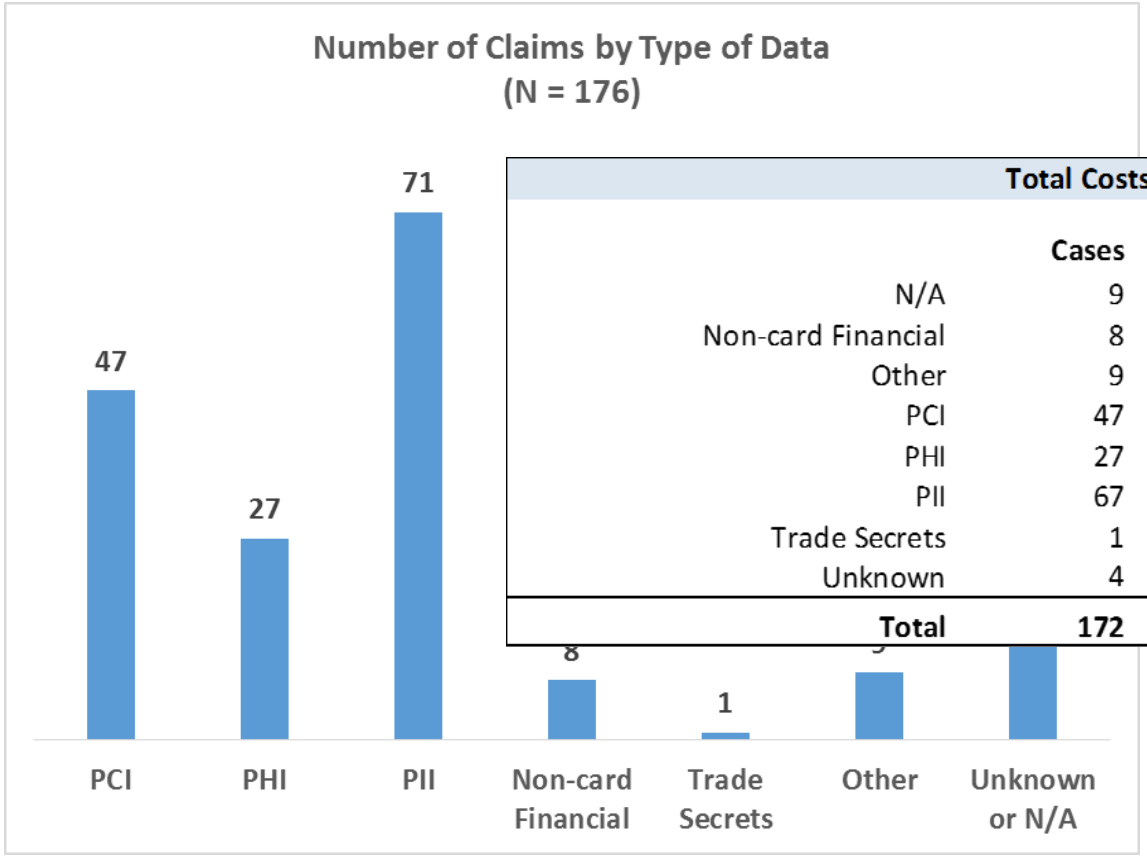


# Security Statistics

Compiled from:
- NetDiligence/McGladrey 2016 Annual Cyber Claims Study

- Utility, Manufacturing, Services
  - New for 2016

*The payout for loss of trade secrets was more than fifty times the median cost of a PCI-related claim.*




**Total Costs (including SIR)**

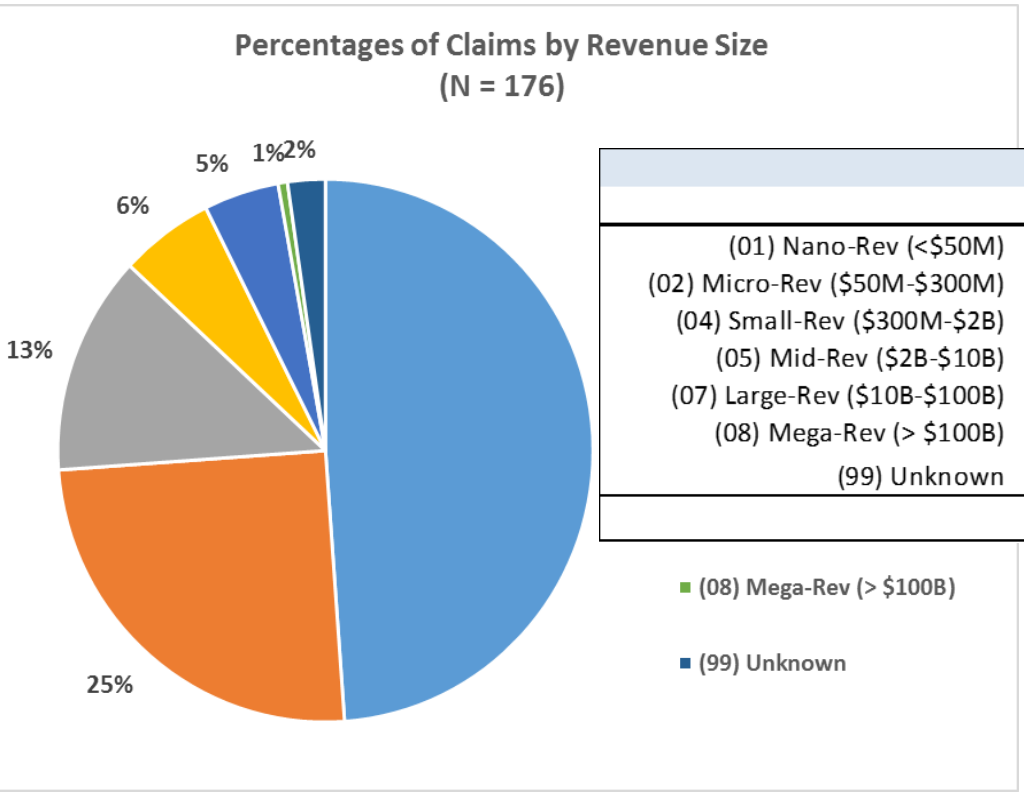
| | Cases | Min | Median | Mean | Max |
|---|---|---|---|---|---|
| N/A | 9 | 14,949 | 52,545 | 183,687 | 1,049,643 |
| Non-card Financial | 8 | 11,280 | 58,633 | 1,545,744 | 11,491,000 |
| Other | 9 | 1,190 | 73,480 | 405,991 | 1,606,550 |
| PCI | 47 | 594 | 93,199 | 894,650 | 10,000,000 |
| PHI | 27 | 290 | 58,851 | 1,515,149 | 15,000,000 |
| PII | 67 | 661 | 50,186 | 125,263 | 917,827 |
| Trade Secrets | 1 | 4,961,000 | 4,961,000 | 4,961,000 | 4,961,000 |
| Unknown | 4 | 26,181 | 67,990 | 89,773 | 196,931 |
| **Total** | **172** | | | | |

# Security Statistics

Compiled from:
- NetDiligence/McGladrey 2016 Annual Cyber Claims Study

- Organization Size
  - New for 2016

*The largest legal costs were from Micro-Revenue organizations. The largest regulatory costs were from the actions of a rogue employee at a Mega-Revenue organization.*




| Total Costs (including SIR) | | | | | |
|---|---|---|---|---|---|
| | Cases | Min | Median | Mean | Max |
| (01) Nano-Rev (<$50M) | 85 | 290 | 49,000 | 215,297 | 7,130,000 |
| (02) Micro-Rev ($50M-$300M) | 44 | 1,000 | 88,154 | 487,411 | 6,570,000 |
| (04) Small-Rev ($300M-$2B) | 23 | 4,178 | 118,671 | 599,907 | 5,650,000 |
| (05) Mid-Rev ($2B-$10B) | 9 | 2,662 | 91,457 | 173,851 | 678,000 |
| (07) Large-Rev ($10B-$100B) | 8 | 1,603,800 | 3,326,313 | 5,965,571 | 15,000,000 |
| (08) Mega-Rev (> $100B) | 1 | 11,491,000 | 11,491,000 | 11,491,000 | 11,491,000 |
| (99) Unknown | 2 | 7,338 | 9,482 | 9,482 | 11,625 |
| | **172** | | | | |

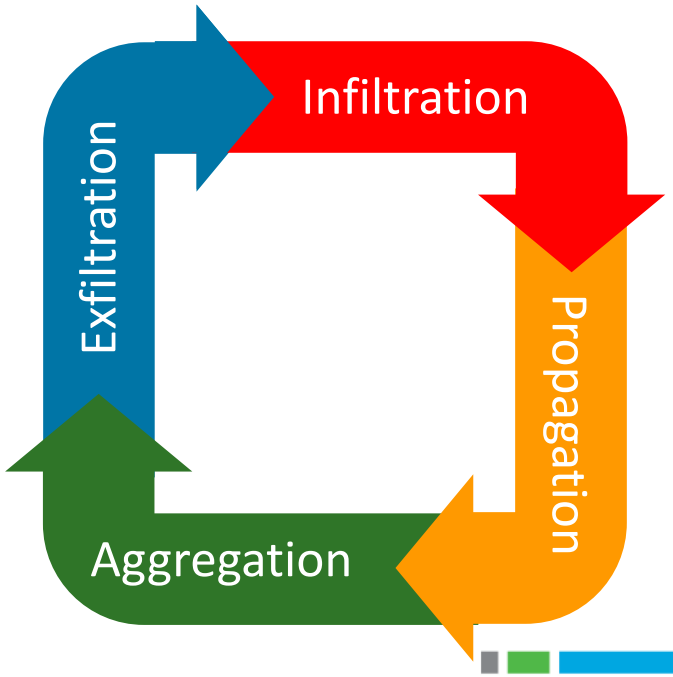
# THROUGH THE MIRROR

aka. It’s not all about you

# Case Study

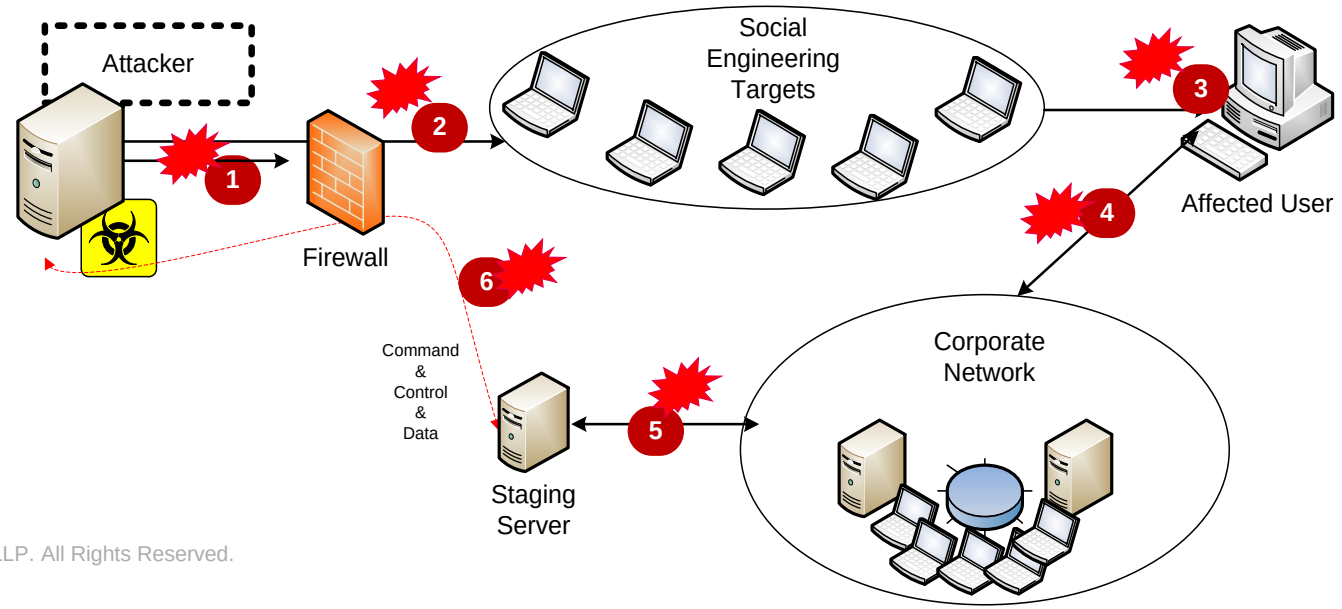
- Attacks are generally carried out in in four stages
- These four stages are often referred to as "The Breach Quadrilateral"

  - Controls must be deployed within the environment that impede your adversary at each stage of the breach cycle
  - Typical defensive focus is on the infiltration stage, but attackers are often most skilled in this area
  - Successful defense is often tied to controls in the later three



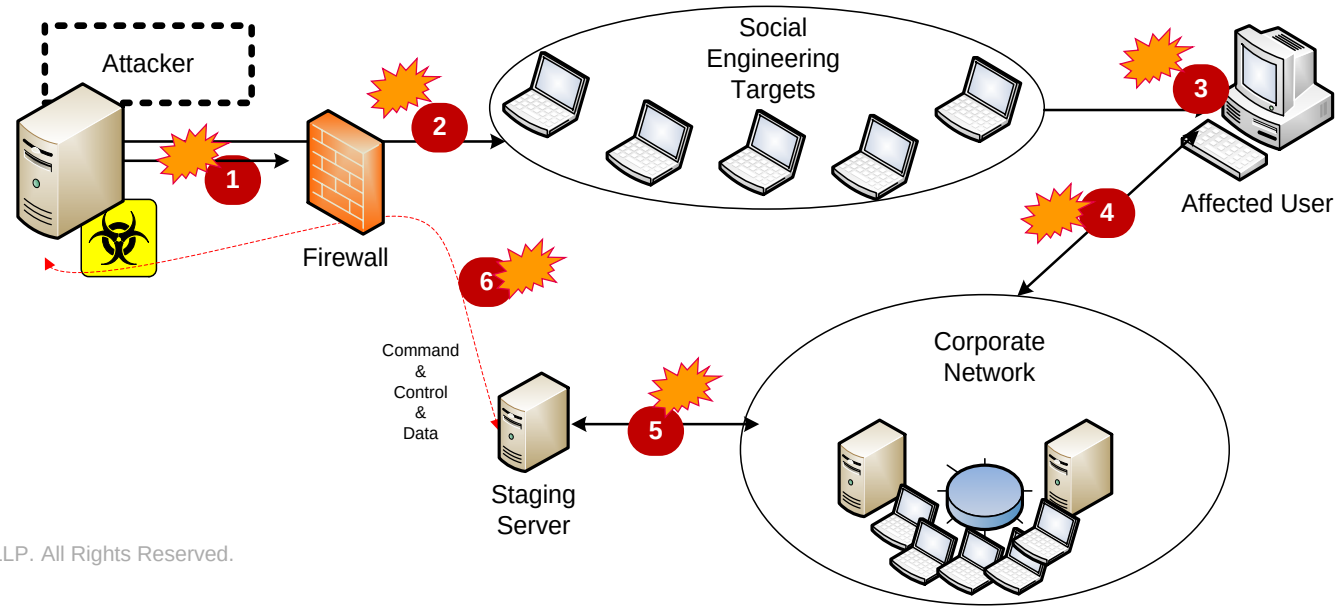
# Case Study – Attack View

1. Attacker scans and attempts exploitation, but fails
2. Attacker utilizes social engineering against a selected population
3. Victim(s) fall for the ruse allowing attacker to enter the environment
4. Attacker leverages user/system access to spread to other systems
5. Attacker consolidates loot (data, passwords, bank access, etc.)
6. Attacker sends data back out of environment



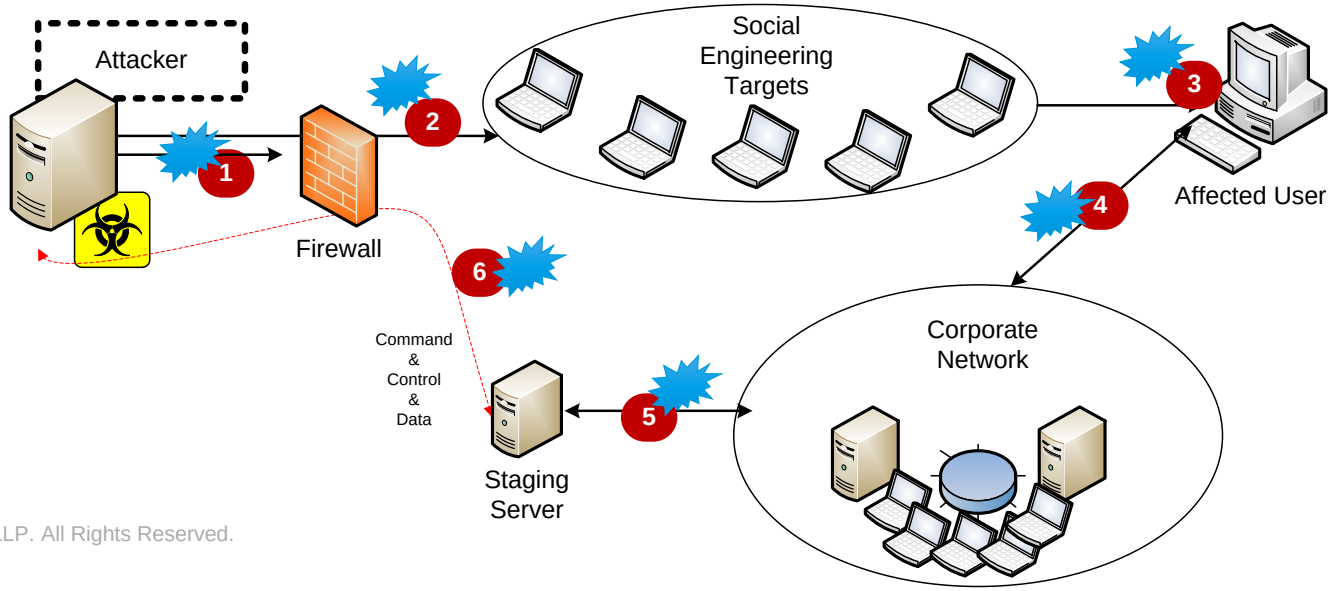
# Case Study – Detective View

1. Firewall and IDS shows exploitation attempts and offending IP
2. Malware gateways and spam filters identify social engineering emails
3. Email logs show affected users, system logs show impact
4. System, network, and domain logs show propagation
5. DLP alerts on sensitive data move, network/system logging of moves, file system monitor flags new files/directories
6. Firewall, IDS, malware gateways alert on suspect traffic, DLP alerts to sensitive data outbound



# Case Study – Corrective View

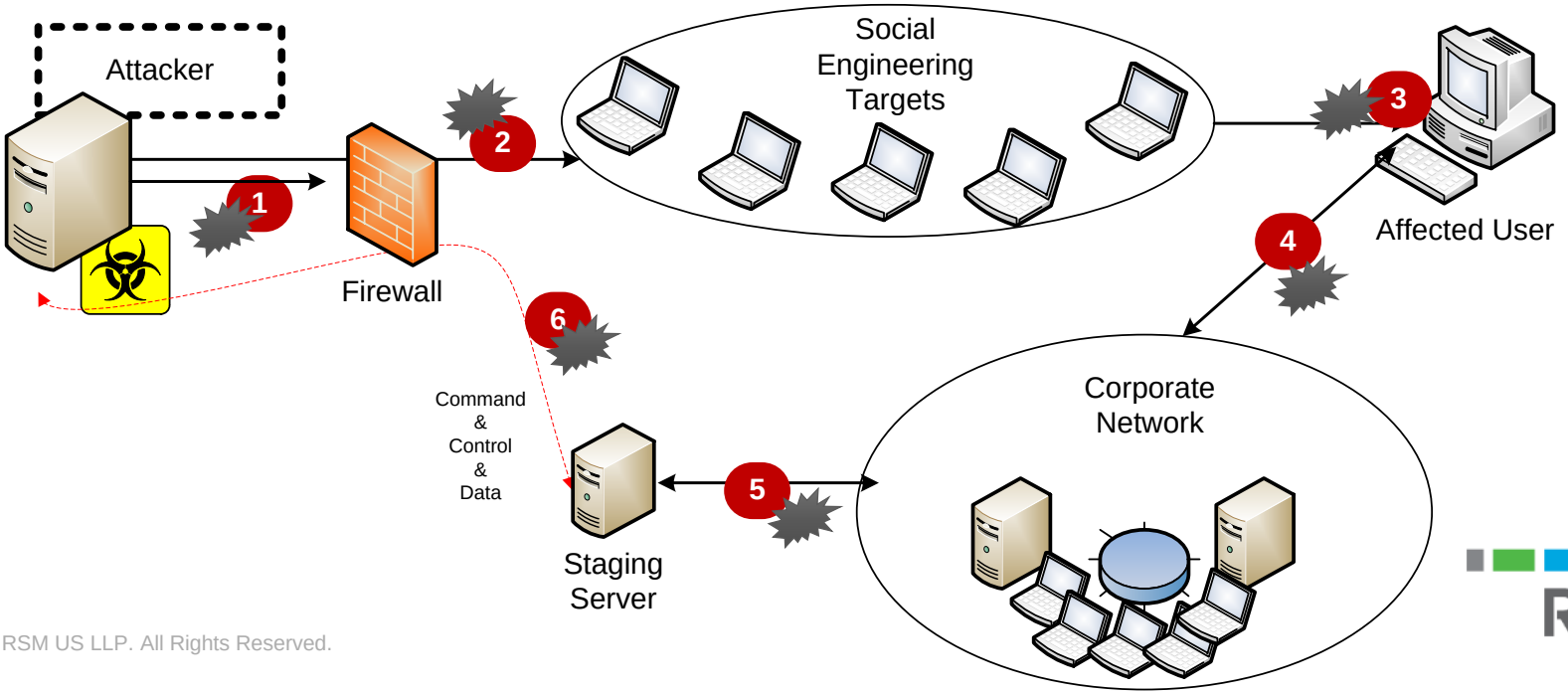
1. Blacklist attacker, add offending IP to custom IDS/SIEM alerts
2. Rapid removal of emails, add embedded outbound IP to alerts, analyze malware from attachments/website and add custom AV alert
3. Isolate/rebuild systems, password resets for affected users
4. Mass password resets, network isolation, limitation to data stores
5. Emergency DLP scans, system/network isolation, enhanced logging
6. Emergency exfiltration changes, retroactive analysis of offending internal and external IPs, initiation of full breach response process



# Case Study – Demo

- Walk through a simple case study from attacker and defender perspectives
- Notice roles flip:
  - Before compromise: Defender can make just one mistake and attacker wins
  - After compromise: Attacker can make just one mistake and defender wins

*If the defender is looking



# Relative Actions – Infiltration Stage

## Organizations often focus majority of their controls on this phase

- Identify and block attackers during initial “foot printing” and exploitation
- Never allow the attackers to gain the full access they need for later stages

| Attack | Detection/Evidence | Corrective Action Type |
|---|---|---|
| External scanning/exploit attempts (Nmap, Nessus, Worms, etc.) | src/dst IP, port, protocol, IDS alerts on specific exploits | Blacklisting, custom IDS/IPS signatures, vulnerability scans, OS/App patch/upgrades |
| Social engineering emails | Email system alerts, DNS information, malware alerts | Email/malware analysis, blacklist source & outbound IPs, removal of emails from all affected users, user notifications |
| Web application/Remote access attacks | Failed logins, src/dst IP, web application logs, web application firewall logs (WAF) | Blacklisting, disable and audit user accounts, WAF custom signatures, web server analysis (files, connections, etc) |
| Denial of service | src/dst IP, port, protocol, IDS alerts | ISP coordination, border router changes, web app changes, DDoS protection providers |

# Relative Actions – Propagation Stage

## The most critical stage, but treated as an operations hygiene issue by most organizations

- When properly constructed early responses can keep an issue as an “event” rather than an “incident”
- Most commonly missed component is the work to identify true issues rather than just symptoms

| Attack | Detection/Evidence | Corrective Action Type |
|---|---|---|
| Password cracking, pass the hash, default passwords, creation of new accounts | System logs, domain logs, authentication sources (e.g. LDAP) | Mass password resets, account disabling, user/password audits, emergency reduction in privileged accounts, enhanced logging |
| Internal exploitation of unpatched systems | Alerts from local protective solutions such as endpoint protection and anti-virus, internal network IDS | System isolation/shutdown, emergency rebuilds, vulnerability scanning + emergency patching/configuration changes |
| Moving into critical areas of networks | src/dst IP/ports, failed access attempts | Emergency change to internal firewalls/ACLs, VLANs, changes to app/user data access |
| Malware infection*<br>• A special case of all above | IDS/malware/firewall alerts, password/DNS changes, outright notifications from malware/attackers | All of the above, malware forensics, custom AV signatures |

# Relative Actions – Aggregation Stage

The stage where the issue transitions from an "event" to an "incident"

- Depending on the law/regulation even if the data is not exfiltrated, attacker access is enough for a "breach"
- Corrective actions are focused on breaking access to data at the source or at the staging point, and/or the attacker's ability to remove it from the environment

| Attack | Detection/Evidence | Corrective Action Type |
|---|---|---|
| Attempts to access sensitive data | Server logs, DLP alerts, database activity, authentication/access logs | Disable offending accounts, password resets, block offending internal IPs, emergency network changes to limit access to data repositories |
| Consolidation of data | Connection logs including quantity of data moved, account activity in server logs, DLP alerts, HIDS file system alerts | Isolation of offending IPs, emergency DLP scans, custom HIDS signatures including file system changes (may identify staging servers), retroactive log reviews (how long has it been occurring? How much is involved?) |

# Relative Actions – Exfiltration Stage

## Exfiltration identification and blocking is your last chance control

- Attack needs to export compromised data (intellectual property, PII, Cardholder Data, corporate financials, etc.)
- Blocking/alerting on these attempts can kill the incident
- Logging the actions can assist in post-breach issues

| Attack | Detection/Evidence | Corrective Action Type |
|---|---|---|
| Command and control | Firewall rejects, GeoIP alerts, malicious IP/domain alerts | Blacklisting, custom IDS/IPS signatures, |
| Exporting stolen data out of the environment | Firewall rejects for outbound filtering, DLP in motion alerts, malicious IP/domain alerts | Full breach response (Technical, Legal, Public Relations, Law Enforcement, Insurance, etc.) |

# NON-TECHNICAL ATTACKS

aka. KISS

# Threat Overview


- Focus for many regulations and industry standards is on “high tech” hacking
- Primary issue in reality is “low tech” hacking that bypass most technical security controls
- Very polished method of social engineering that does not require actual “hacking”
- Fancy name for traditional “con games”
  - Attacking an environment via manipulating people

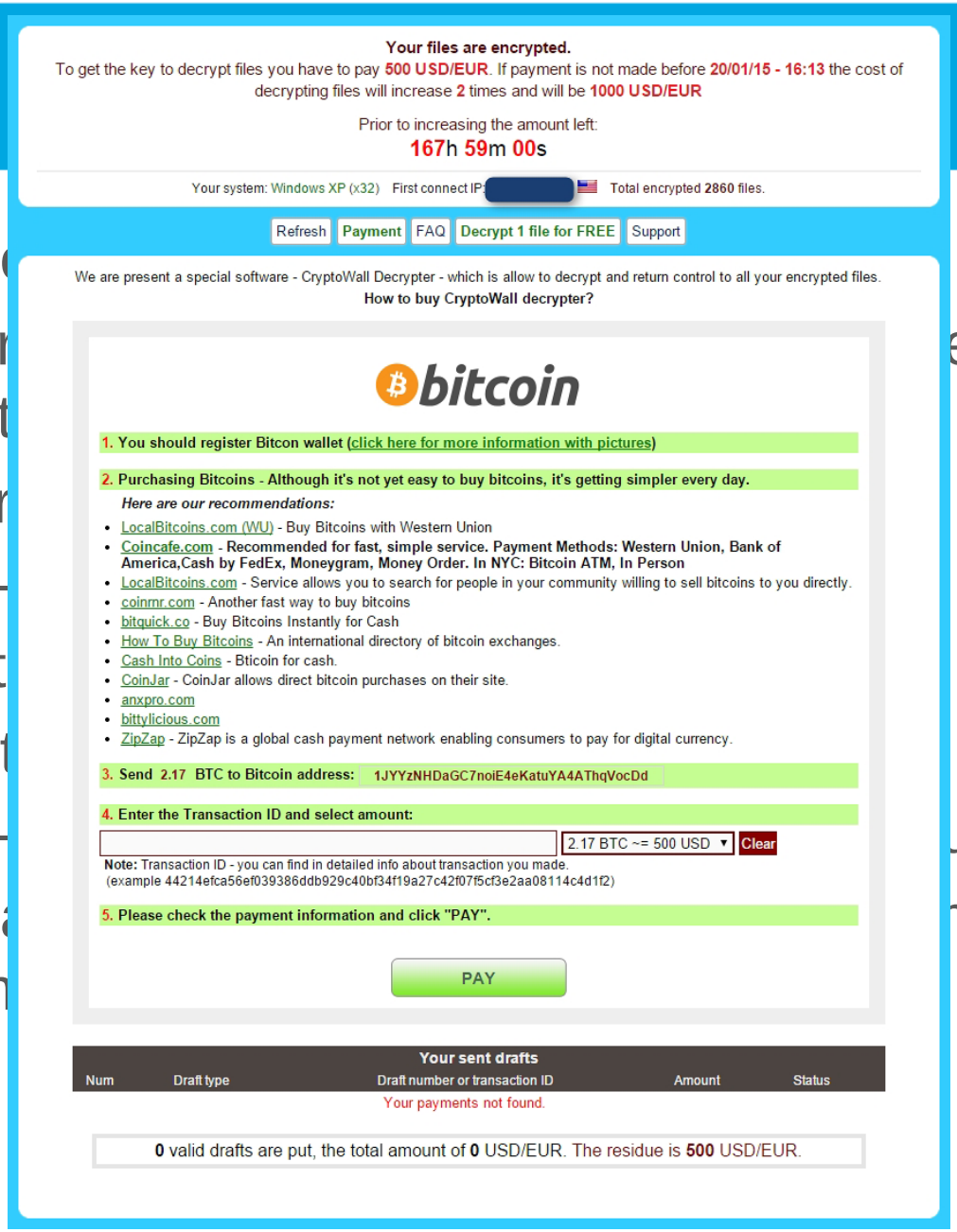
# Threat

- Ranso
- Either
  - Cr
  - St
  - Int
  - Ma

e or threat

ufacturing

mers, en



# Threat Overview

Hello,

To introduce ourselves first
http://www.coindesk.com/bit
http://bitcoinbountyhunter.
http://cointelegraph.com/
coin-theft-owner-accuses-
Or just google "DD4BC" a

So, it's your turn! All
under DDoS attack unless
YgrQ Please note that it
rent UDP flood power is 4
attack on one of your IP
try not to crash it at t
we are serious.

We are aware that you pr
you 24 hours to get it a
coins.info or localbitco
address, you don't even
250 USD, so we are cheap, a

IMPORTANT: You don't even h
dyMump5MiYgrQ – we will kno
We say it because for big c
that there is proof that th

If you need to contact us,
if you ignore us, and don't
to stop will go to 100 BTC
of our "clients" believe th
we work - we never attack the same target after we are paid. If you are thinking
about reporting this to authorities, feel free to try. But it won't help. We are
not amateurs.

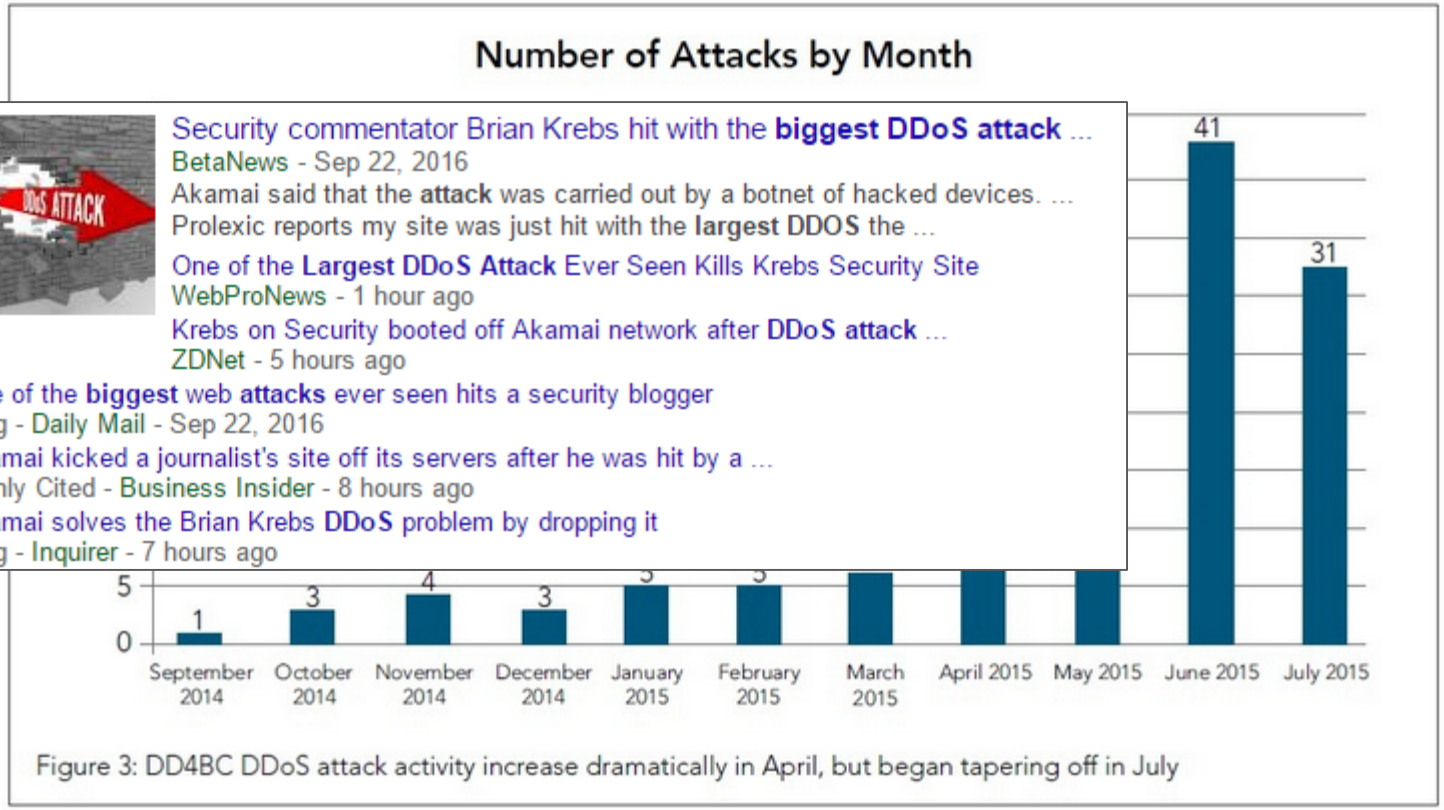


Figure 3: DD4BC DDoS attack activity increase dramatically in April, but began tapering off in July

- DD4BC attacks have increased dramatically over the last few months Source: Akamai

# Threat Overview

- Vendor Fraud aka. Invoice Fraud aka. Supply Chain Fraud:
  - Attacker identifies a vendor of the organization
  - Attacker attempts to convince the organization to make a normal or additional payment to a new account
  - Organization unaware of fraud until notified by the vendor
  - Typical example:

To: [Someone in finance]
From: Executive@vend0r.com
Sent: Mon, Oct 5, 2015 at 2:01am

Mr/Mrs. Someone, please be aware that we have recently changed banking providers. Our new account and routing numbers are in the attached pdf.
Respectfully, Mr. Vendor Executive

# Threat Overview

- Fake Executives:
  - Often create entire fake email chains including supposed communications with other executives
  - May tie to fake vendor claims, but also tax payments, legal fines, issuing corporate credit cards, fake checks, etc.
  - Utilizes organizational and positional pressure to succeed
  - Typical Example:

To: [Someone in finance]
From: Executive@ourc0mpany.com
Sent: Mon, Oct 5, 2015 at 2:01am

Hey, [nickname]. I was just contacted by one of our key vendors and it looks like we missed a payment last month. We are currently negotiating next year's contract so this is VERY sensitive. Immediately wire $xxx,xxx to the attached account information or there will be hell to pay for all of us.
Respectfully, CEO Executive

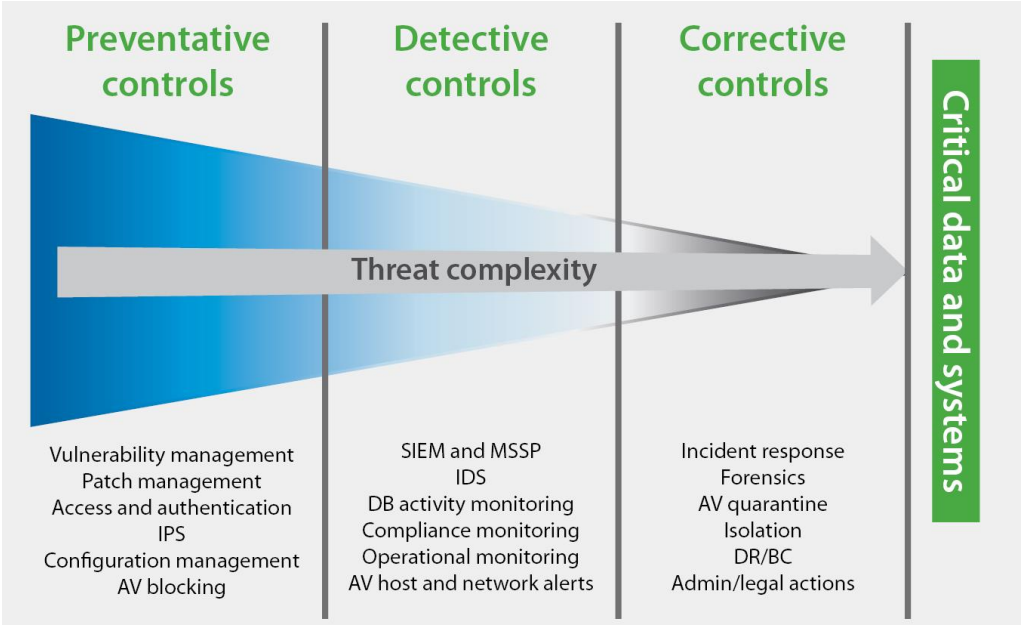
# RECOMMENDATIONS

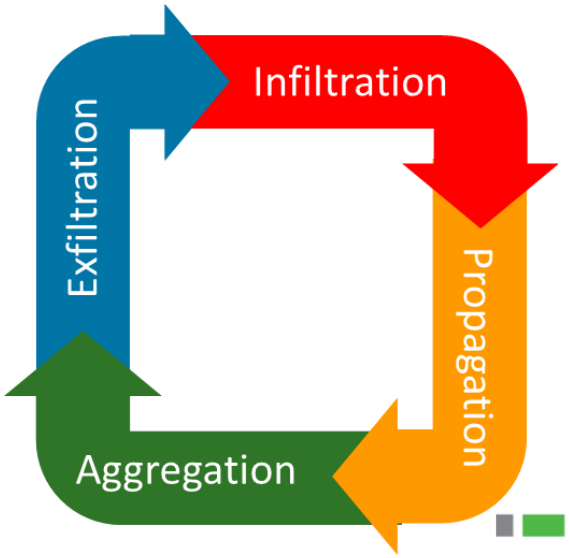
# Recommendations

Make sure you have basic controls in 3 layers

- Prevent → Detect → Correct
- Have you made yourself a hard target?
- Are you capable of knowing if you have been breached?
- Can you respond effectively?

Deploy each type of control for each phase of the breach quadrilateral



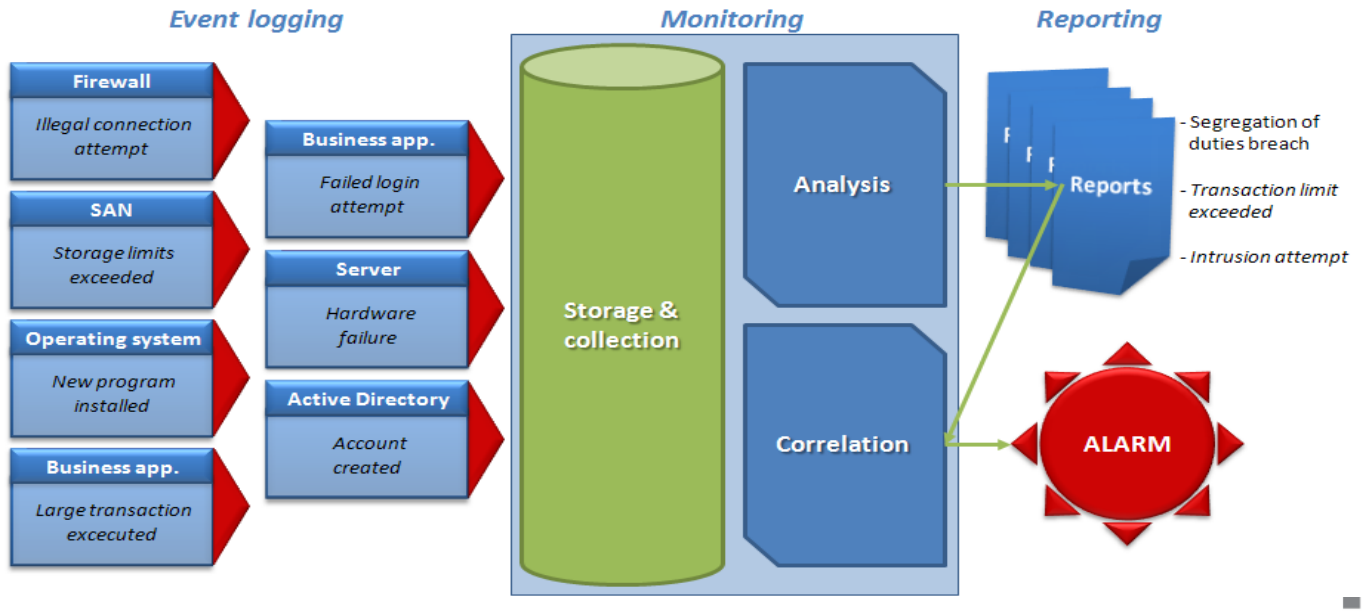

RSM

# Recommendations
*Low-Tech Hacking*

- Payment controls
  - Offline vendor contact lists
  - Multiple approvals
  - AUP for emergency payments including out-of-band communications, executive PINs/Passwords, etc.
- Account Takeovers
  - Two factor authentication
  - Multiple terminals used for multiple approvals
  - Payment limits without verbal approvals
- Ransom
  - Backups of critical data on a frequent basis
  - Arranged DDoS protection with vendor and ISP
  - Pre-determined course of action for payment or non-payment

# Recommendations
## *Monitoring*

- So what do we do?
  - Heavy focus on consolidated security monitoring
  - Log more. Bring it together. Use it. Period.
  - “87% percent of victims had evidence of the breach in their log files, yet missed it.“ Verizon Data Breach Report



# Recommendations
*Incident Response*

- 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…"



RSM

# Recommendations

- Insurance
- The last line of defense
- Do you have cyber insurance?
  - Don’t count on it being covered under your general policy
- Do they cover the common costs?
- Are the sub-limits reasonable?
- Have you complied with all of the covenants?
  - Mapped security policy, IR plan, IR exercise, Security testing, Security monitoring, etc.
- Are your forensic and legal providers approved?

**Daimon Geopfert**
National Leader - Security & Privacy Services

**RSM US LLP**
2000 Town Center, Suite 1900, Southfield, MI 48075

**D:** (312) 634-4523

**M:** (248) 802-4908
**E:** Daimon.Geopfert@rsmus.com