EXTRA, EXTRA! Read all about Cybercrime and your Bank!

IOWA Real BANKERS 2015 CONVENTION

SECURE BANKING SOLUTIONS

SBS

Presented by:
Jon Waldman, SBS – CISA, CRISC

Contact Information

- Jon Waldman
  - Partner, Senior IS Consultant
  - CISA, CRISC
  - Masters of Info Assurance - DSU
  - Phone: 605-380-8897
  - Mission: To Save the World!
  - jon@protectmybank.com
  - www.protectmybank.com

My Experience

- 9 Years Information Security
- Information Security Program Design and Implementation
- IT Risk Assessment
- Penetration Testing
- Vulnerability Assessments
- Awareness Programs
- Vendor Management
- Business Continuity
- Technology Selection
- Info Security Consulting

- IT Audit
  - ISP audit
  - Controls audit
  - Wire transfer audit
  - Internet banking audit
- Anything else you can imagine!

SECURE BANKING SOLUTIONS SBS

Dakota State Nationally Recognized

- National Security Agency
- Department of Homeland Security
- 4,000 universities in the country
- Only 100 named national centers in the past 10 years
- National Center of Excellence in Information Assurance
- www.dsu.edu

Cybersecurity State of the Union

- Trends (new tech, greater adoption)
- 2014 – Year of the Data Breach
- New and widespread vulnerabilities
- Cybercrime – increasing rapidly!
- Commercial Account Takeover
- New Regulatory Guidance
  - Two new Joint Statements
  - Cybersecurity Assessments

I CHANGED ALL MY PASSWORDS TO "INCORRECT".
SO WHENEVER I FORGET, IT WILL TELL ME "YOUR PASSWORD IS INCORRECT."
TROLL.ME

Why are we talking about this?

- Where's your data?
- Who's ultimately responsible for your data?
- Where is information trending?
- Is this whole "world wide web" thing a fad?

SO YOU THINK THIS INTERNET THING IS A FAD?
TELL ME AGAIN HOW WELL THE YELLOW PAGES ARE WORKING FOR YOU.

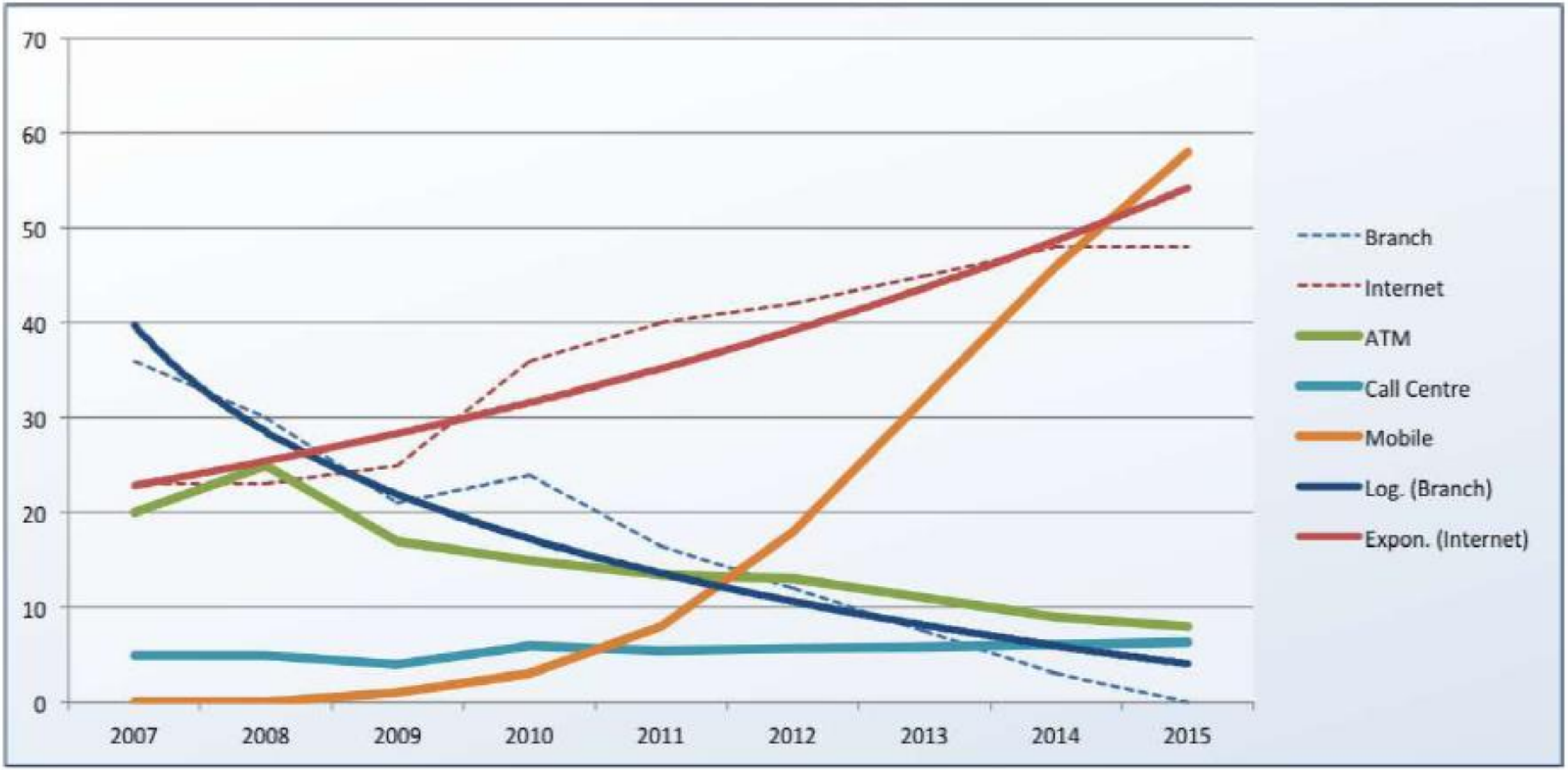
Technology Trends

- Remote Banking
  - Consumer Online Banking
  - Commercial Online Banking
  - Mobile Banking
- Mobile Payments
  - Mobile Deposit Capture
  - Commercial Mobile Deposit
  - P2P Payments
- Interactive Teller Machines
- Contactless Payments
- Increased Outsourcing
- Data Breaches…

Digital Banking Trends

- More or less access to money digitally?
  - $96,000 of sales are made on Amazon every minute
  - $612,000 is spent online by consumers every minute
  - http://www.retale.com/info/retail-in-real-time/
- More or less in-person customer interaction?
- Greater or fewer brick-and-mortar locations?
- More or less employees?
- More or less investment into technology?

Banking Method Trends

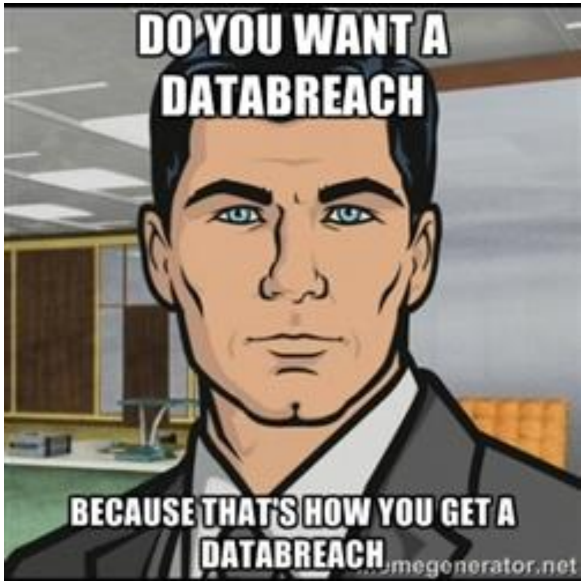


Changes in the Paradigm

“**Banking is quickly changing from a place you go to something you do everyday**,” stated Brett King, author of bestselling “Bank 2.0” and “Bank 3.0,” as well as founder of mobile banking start-up Movenbank

Data Security Issues

- Data Breaches
  - Target, Home Depot, so many more
- Widespread Vulnerabilities
- Cybercrime – who are the new bad guys?
  - Social Engineering using (Malware/Phishing)
  - DDOS
- ATM Security Issues
- Wire Fraud
  - Fraud from within the Bank
- Corporate Account Takeover
  - Fraud from outside the Bank

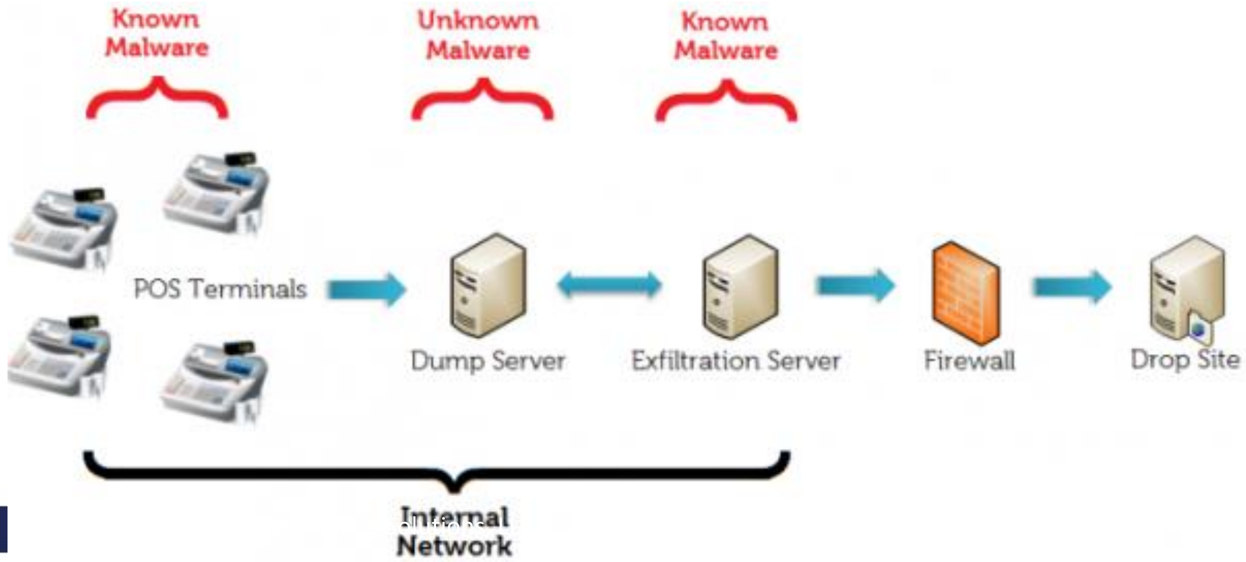


Verizon DATA BREACH INVESTIGATIONS REPORT (DBIR)

- 1367 confirmed data breaches (2014)
- 63,437 security incidents (2014)
- 92% stemmed from **external agents**
  - Organized criminal group 55%
- 55% utilized some form of **hacking**
- 29% utilized some form of **social engineering**
- 40% incorporated **malware**
- 75% of victims were **opportunistic attacks**
- 97% of breaches were avoidable through simple or intermediate controls (*2012)

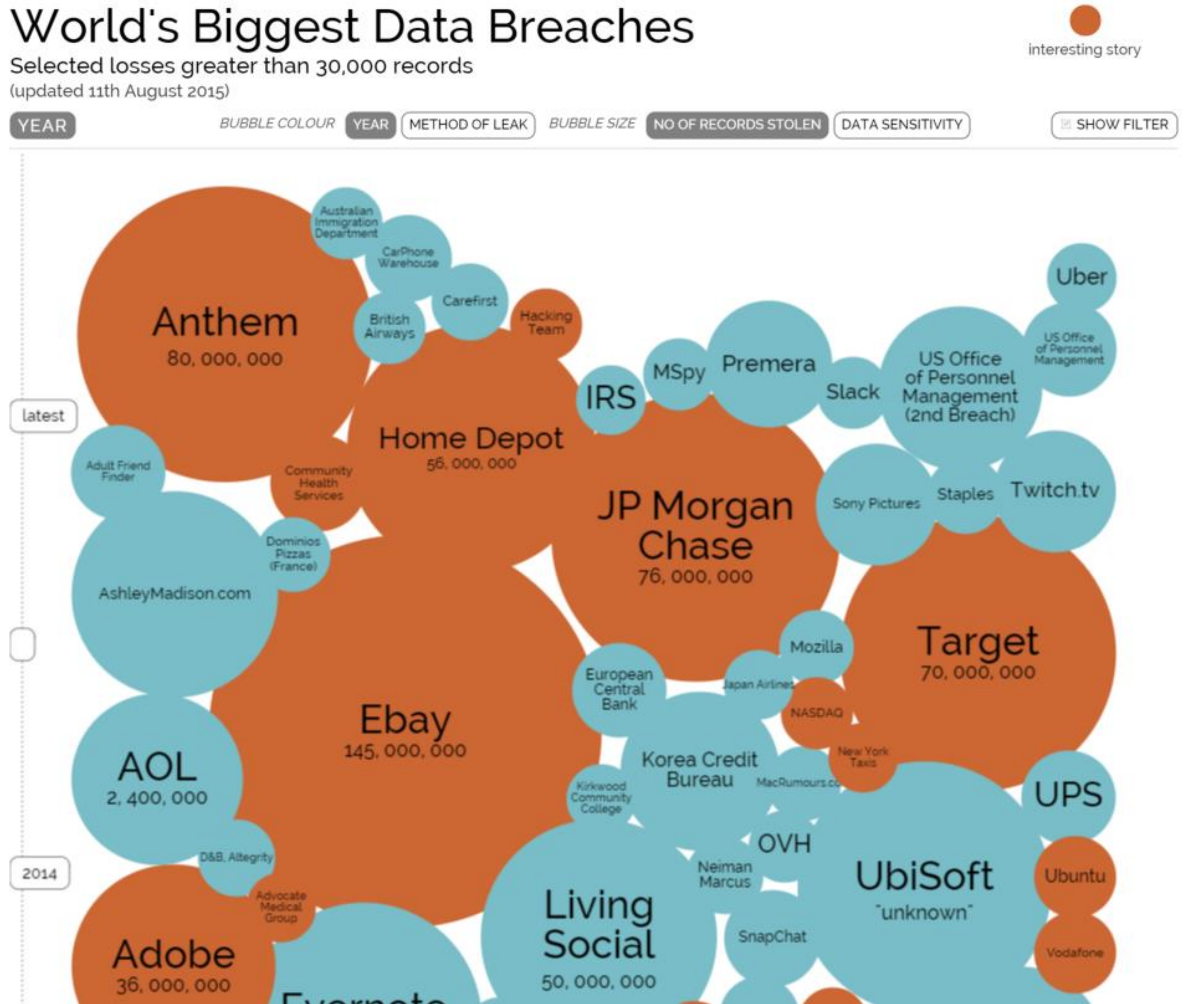
Target (Nov/Dec 2013)

- 40M Credit/Debit Cards
  - Card data for sale online.
- 70M Customer Records
  - names, mailing addresses, phone numbers or email addresses
- Malware-laced email phishing attack sent to employees at an HVAC firm (which supported Target)
- From HVAC company, accessed Target's "Vendor Portal"
- Jumped inside the network and infected many Point of Sale systems



Home Depot (April/Sept 2014)

- Up to 56,000,000 customer records exposed
- Ongoing investigation (full extent not yet known)
- Target = 18 days; Home Depot = 6 months
  - Heartland/TJX = 18 months; 6 months to report
- 2,200 physical store locations affected
- Reportedly the same malware and the same (Russian) cybercrime group responsible



World's Biggest Data Breaches

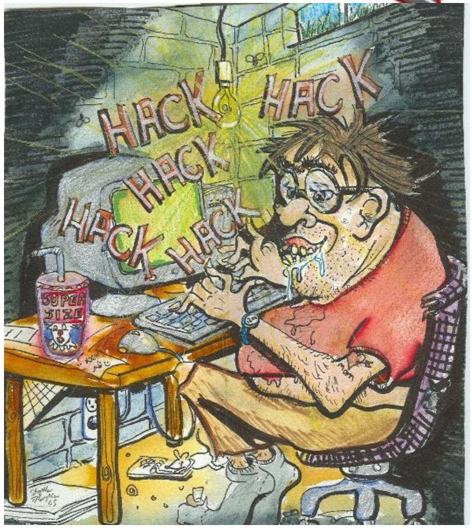
Selected losses greater than 30,000 records

(updated 11th August 2015)

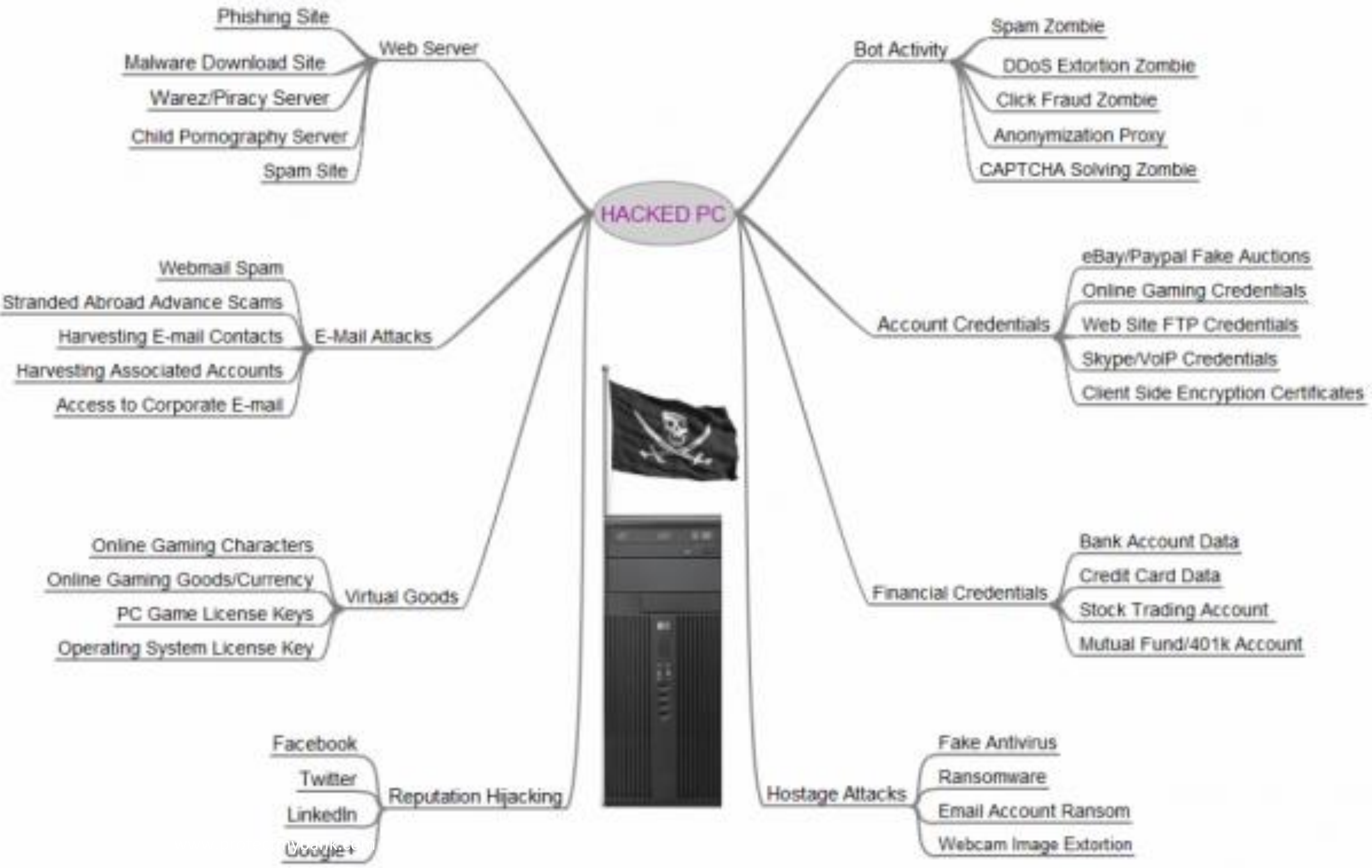
The future of vulnerabilities…?

The evolution of Cyber Crime

- Used to be the “hacker”
- Now, it’s Organized Crime
  - Overseas operations
  - Want $$$ to fund their organization
  - Using Low Tech Attacks
  - Target PEOPLE
  - They purchase specialized software
  - Marketing Material



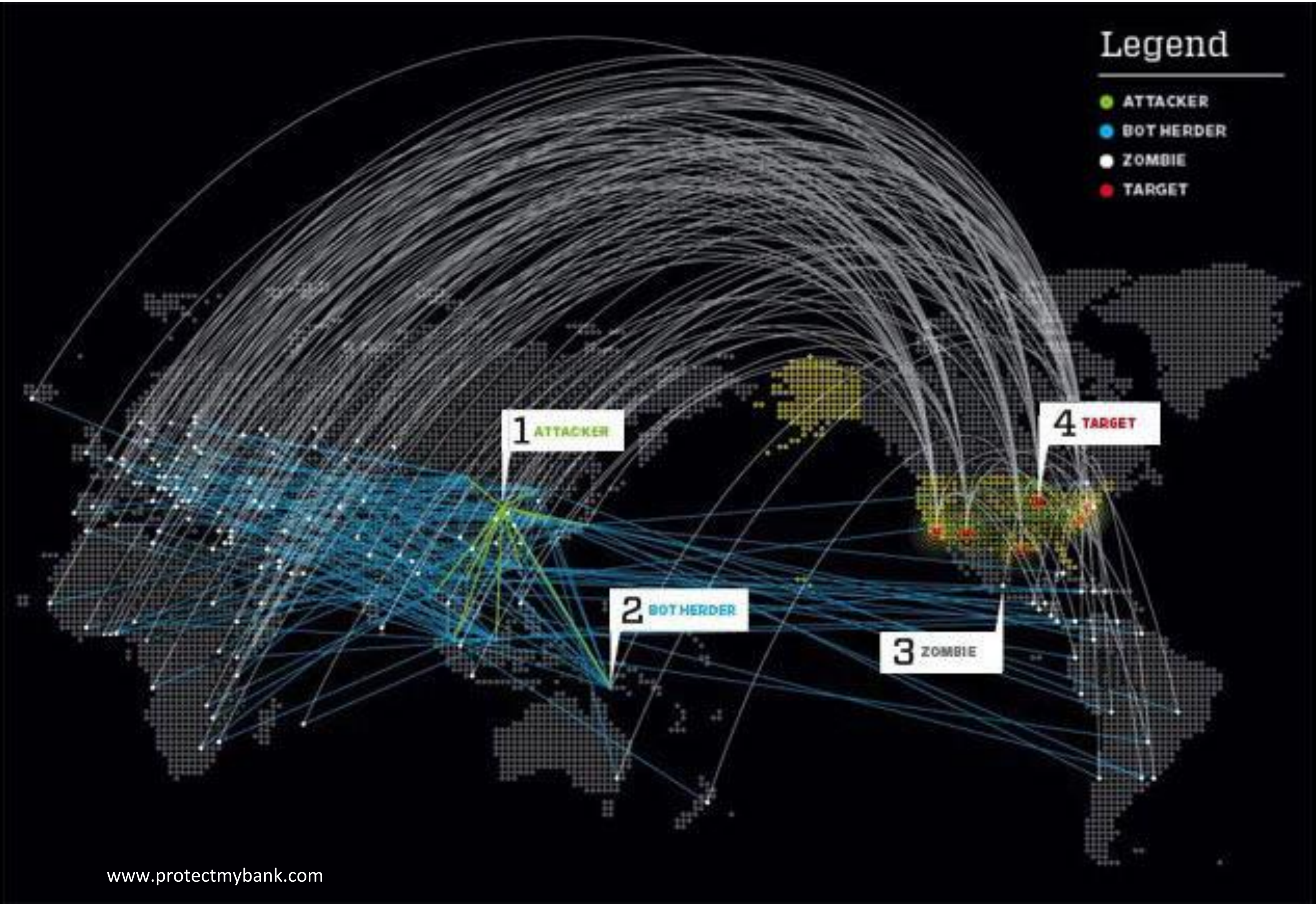
Value of Hacked PC



HACKED PC

- Web Server
  - Phishing Site
  - Malware Download Site
  - Warez/Piracy Server
  - Child Pornography Server
  - Spam Site
- Bot Activity
  - Spam Zombie
  - DDoS Extortion Zombie
  - Click Fraud Zombie
  - Anonymization Proxy
  - CAPTCHA Solving Zombie
- E-Mail Attacks
  - Webmail Spam
  - Stranded Abroad Advance Scams
  - Harvesting E-mail Contacts
  - Harvesting Associated Accounts
  - Access to Corporate E-mail
- Account Credentials
  - eBay/Paypal Fake Auctions
  - Online Gaming Credentials
  - Web Site FTP Credentials
  - Skype/VoIP Credentials
  - Client Side Encryption Certificates
- Virtual Goods
  - Online Gaming Characters
  - Online Gaming Goods/Currency
  - PC Game License Keys
  - Operating System License Key
- Financial Credentials
  - Bank Account Data
  - Credit Card Data
  - Stock Trading Account
  - Mutual Fund/401k Account
- Reputation Hijacking
  - Facebook
  - Twitter
  - LinkedIn
  - Google+
- Hostage Attacks
  - Fake Antivirus
  - Ransomware
  - Email Account Ransom
  - Webcam Image Extortion

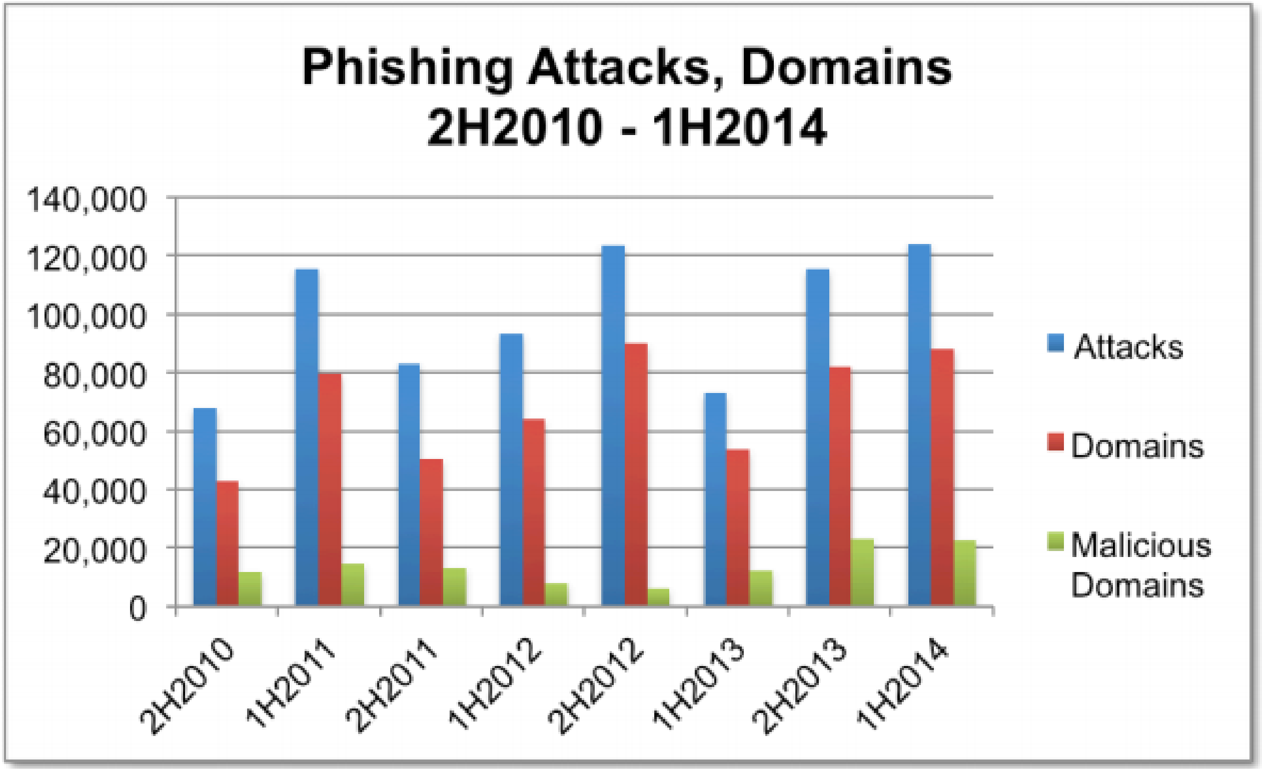
DDoS



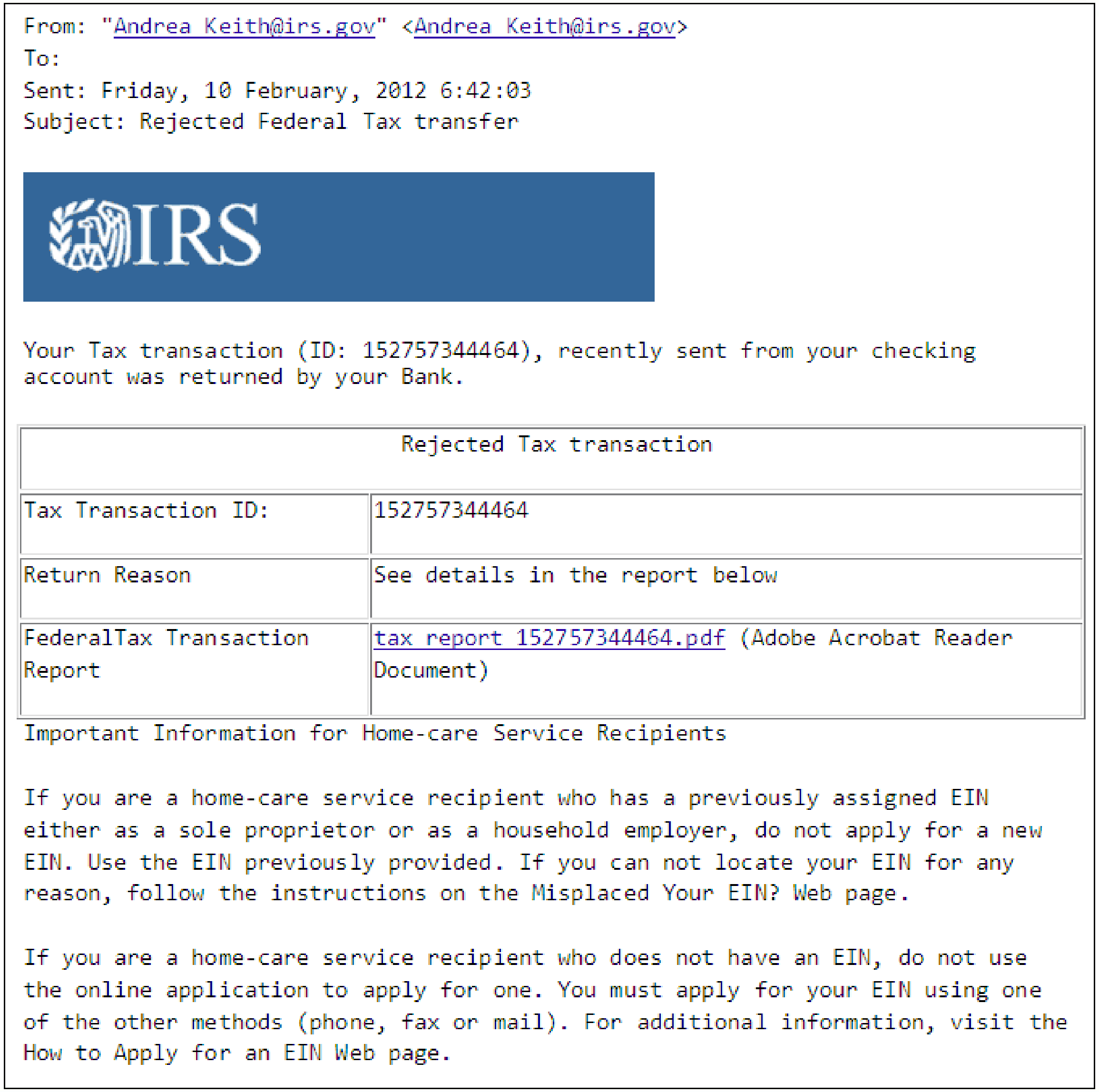
www.protectmybank.com

Phishing Trends

91% of cyberattacks and the resulting data breach begin with a “spear phishing” email – Trend Micro



Phishing… for “low hanging fruit”



From: "Andrea_Keith@irs.gov" <Andrea_Keith@irs.gov>
To:
Sent: Friday, 10 February, 2012 6:42:03
Subject: Rejected Federal Tax transfer

IRS

Your Tax transaction (ID: 152757344464), recently sent from your checking account was returned by your Bank.

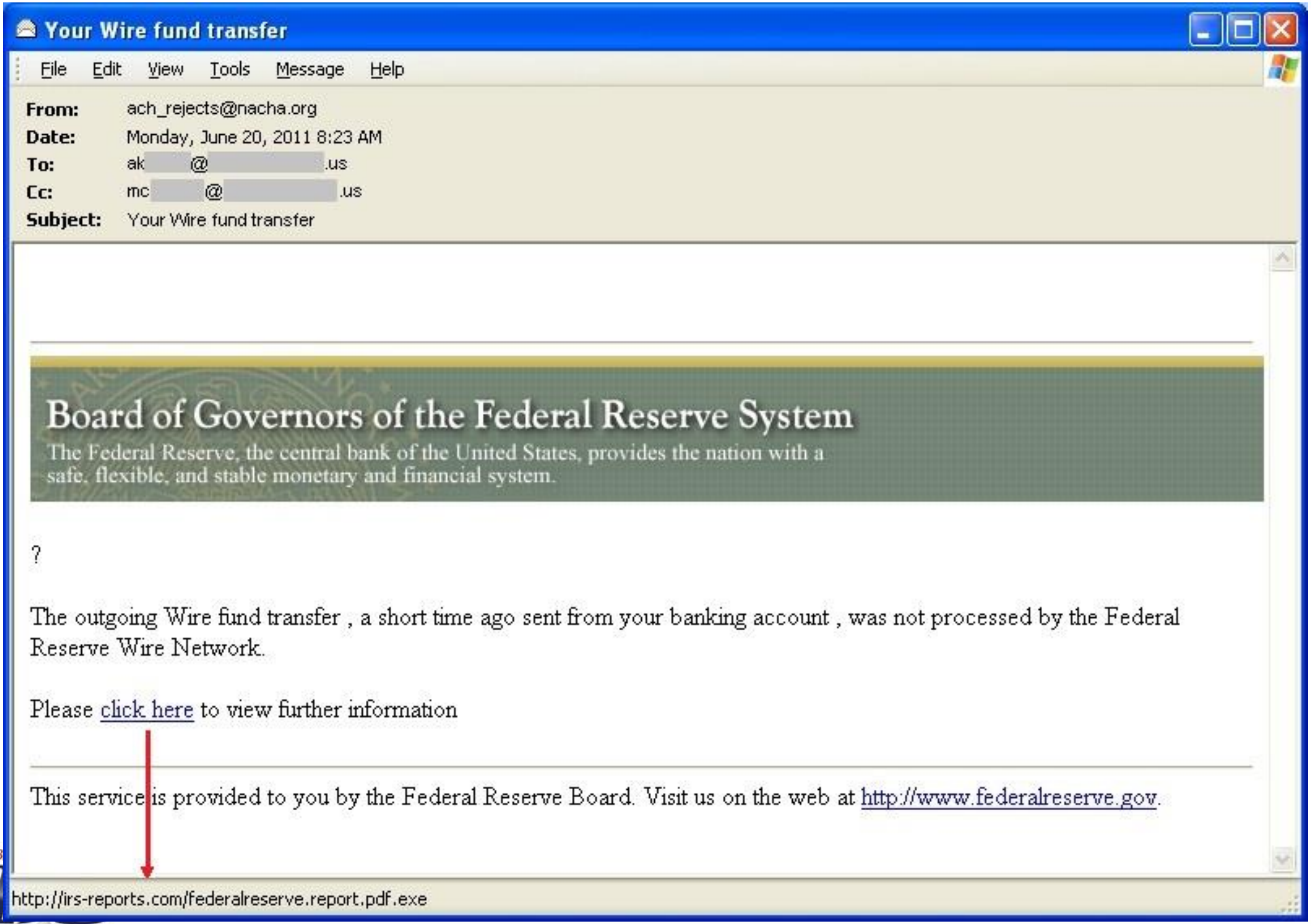
Rejected Tax transaction	
Tax Transaction ID:	152757344464
Return Reason	See details in the report below
FederalTax Transaction Report	tax_report_152757344464.pdf (Adobe Acrobat Reader Document)

Important Information for Home-care Service Recipients

If you are a home-care service recipient who has a previously assigned EIN either as a sole proprietor or as a household employer, do not apply for a new EIN. Use the EIN previously provided. If you can not locate your EIN for any reason, follow the instructions on the Misplaced Your EIN? Web page.

If you are a home-care service recipient who does not have an EIN, do not use the online application to apply for one. You must apply for your EIN using one of the other methods (phone, fax or mail). For additional information, visit the How to Apply for an EIN Web page.

Spear Phishing



From: ach_rejects@nacha.org
Date: Monday, June 20, 2011 8:23 AM
To: ak[redacted]@[redacted].us
Cc: mc[redacted]@[redacted].us
Subject: Your Wire fund transfer

Board of Governors of the Federal Reserve System

The Federal Reserve, the central bank of the United States, provides the nation with a safe, flexible, and stable monetary and financial system.

?

The outgoing Wire fund transfer , a short time ago sent from your banking account , was not processed by the Federal Reserve Wire Network.

Please click here to view further information

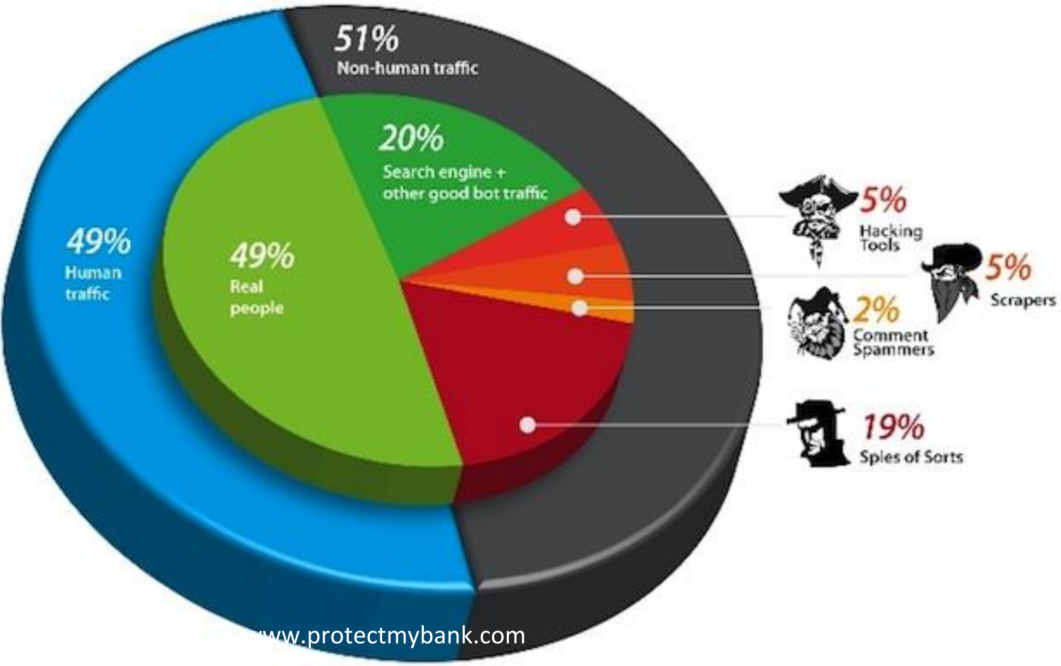
This service is provided to you by the Federal Reserve Board. Visit us on the web at http://www.federalreserve.gov.

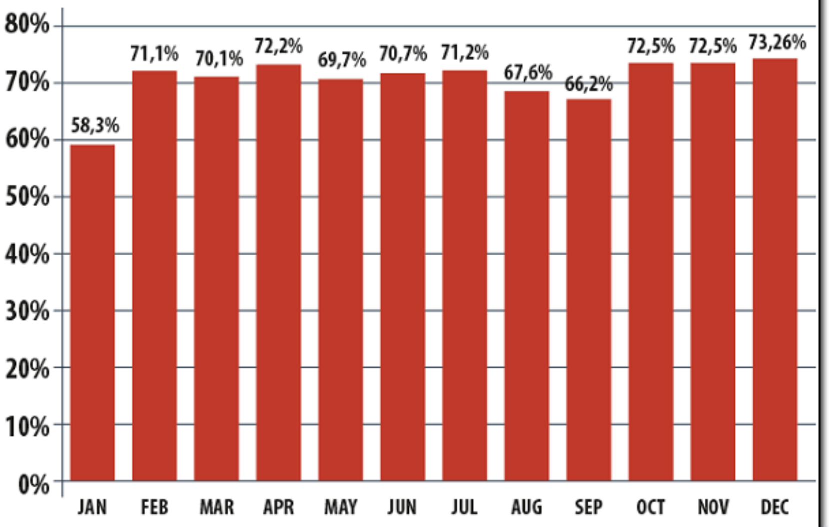
http://irs-reports.com/federalreserve.report.pdf.exe

Threats to Small Businesses

Q2: Scanned Computers	18,321,456	
Infected Computers	9,215,692	50.30%
Non Infected Computers	9,105,764	49.70%
Banking Trojans / Password	3,220,911	17.58%
Downloaders	1,533,506	8.37%

"if you click a malicious link or open an attachment in one of these emails, there is less than a **one-in-five chance your antivirus software will detect** it as bad." - Krebs





Wire Fraud vs. CATO

Wire Transfer Fraud – INTERNAL

- a new trend in which cyber criminals are using spam and phishing e-mails, keystroke loggers, and Remote Access Trojans (RAT) to compromise financial institution networks and obtain employee login credentials.
- Amounts varied between $400k and $900k
- Raised the wire transfer limit on the customer's account to allow for a larger transfer
- Most of the identified wire transfer failures, the actor(s) were only unsuccessful because they entered the intended account information incorrectly

Wire Fraud vs. CATO

Commercial Account Takeover - EXTERNAL

- Cyber criminals are targeting small businesses
- Small businesses don't have security controls in place!
- Small businesses are using Internet Banking - Cash Management systems
  - Bill Pay, Wire Transfers, Direct Deposit, Mobile Capture, etc.
- Cyber criminals take over small business internet banking accounts and transfer money
- CATO = bad news bears for everyone involved

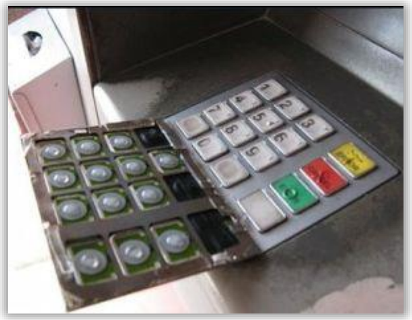
Commercial Banking Fraud

- **Chelan County Public Hospital** (WA) lost $1.03 Million after attackers accessed payroll accounts and transferred the money into 96 different bank accounts
- **JT Alexander & Son**, a North Carolina fuel distributor lost $800,000 in May 2014 due to fraudulent ACH transfers initiated via Commercial Online Banking
- **Experi-Metal Inc.** of Sterling Heights, MI had $1.9M stolen, of which $560,000 was not recoverable due to 47 wires in one day to foreign and domestic accounts which EMI never wire to before
- **PATCO Construction** of Maine lost more than $500,000 due to Commercial Account Takeover in 2009 (probably the most public and infamous case, due to the lawsuits and outspoken owner)
- **Choice Escrow and Land Title** of Missouri lost $440,000 due to fraudulent wire transfers in 2009; courts ruled in favor of Bank in March of 2013, stating that the Bank had offered "commercially reasonable security" to Choice Escrow, but the business turned down the additional security features.
- So many more!

ATM Security

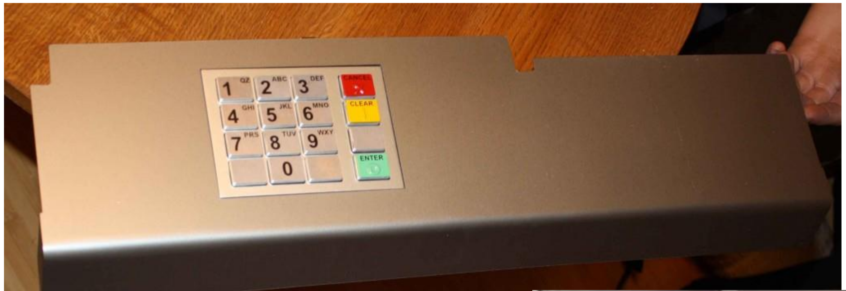
- ATM security is SO HOT right now.
- Do your ATMs use Windows XP?
- Have you addressed other ATM threats?
  - Skimming
  - Cash-out
  - Malware
  - Physical Security

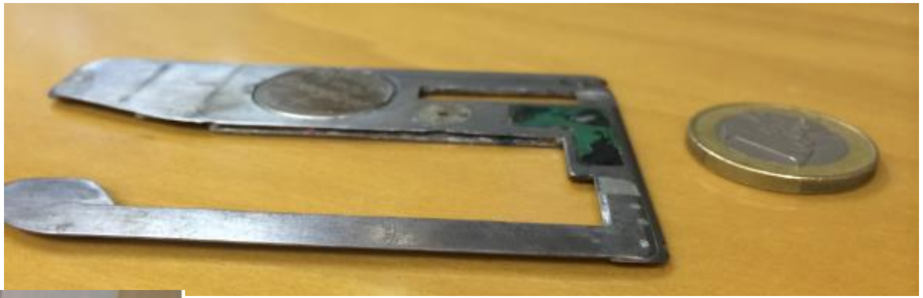
Latest Skimming Techniques

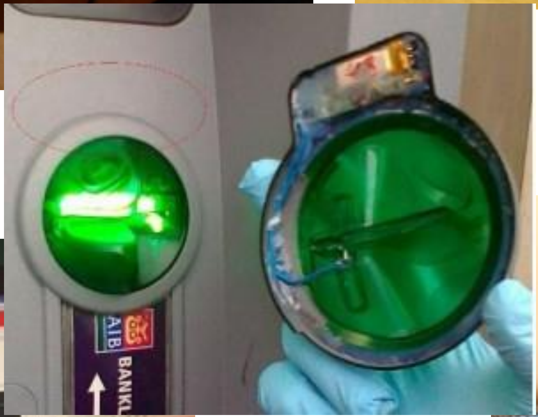


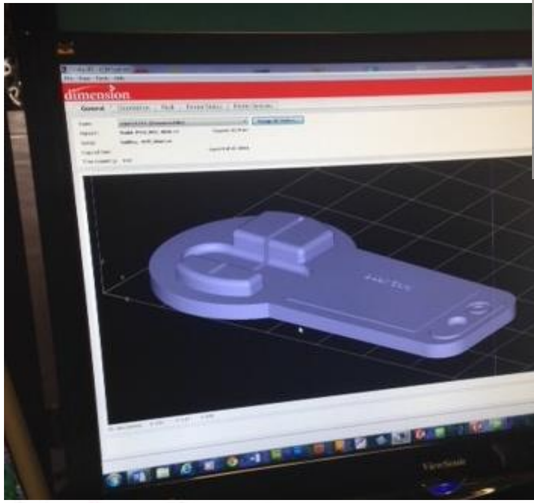
- Completely Fake ATM’s and ATM covers.
- Keypad overlay instead of camera’s.
- Transmission devices: cell phone, Wi-Fi, Bluetooth…
- Gluing down the physical ‘enter’, ‘cancel’ and ‘clear’ keys. Allowing hacker to capture PIN and get the card.
- Card/Cash Trapping
- http://krebsonsecurity.com/all-about-skimmers/

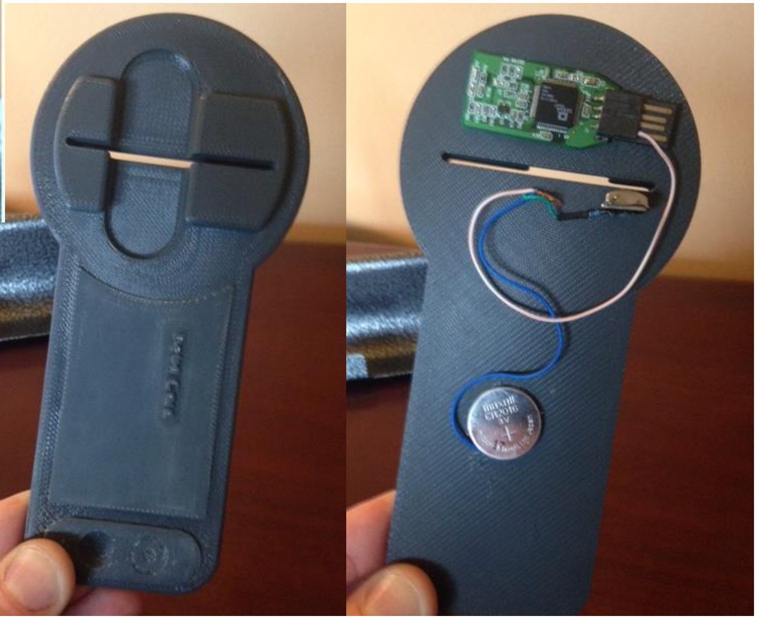
Skimming examples…



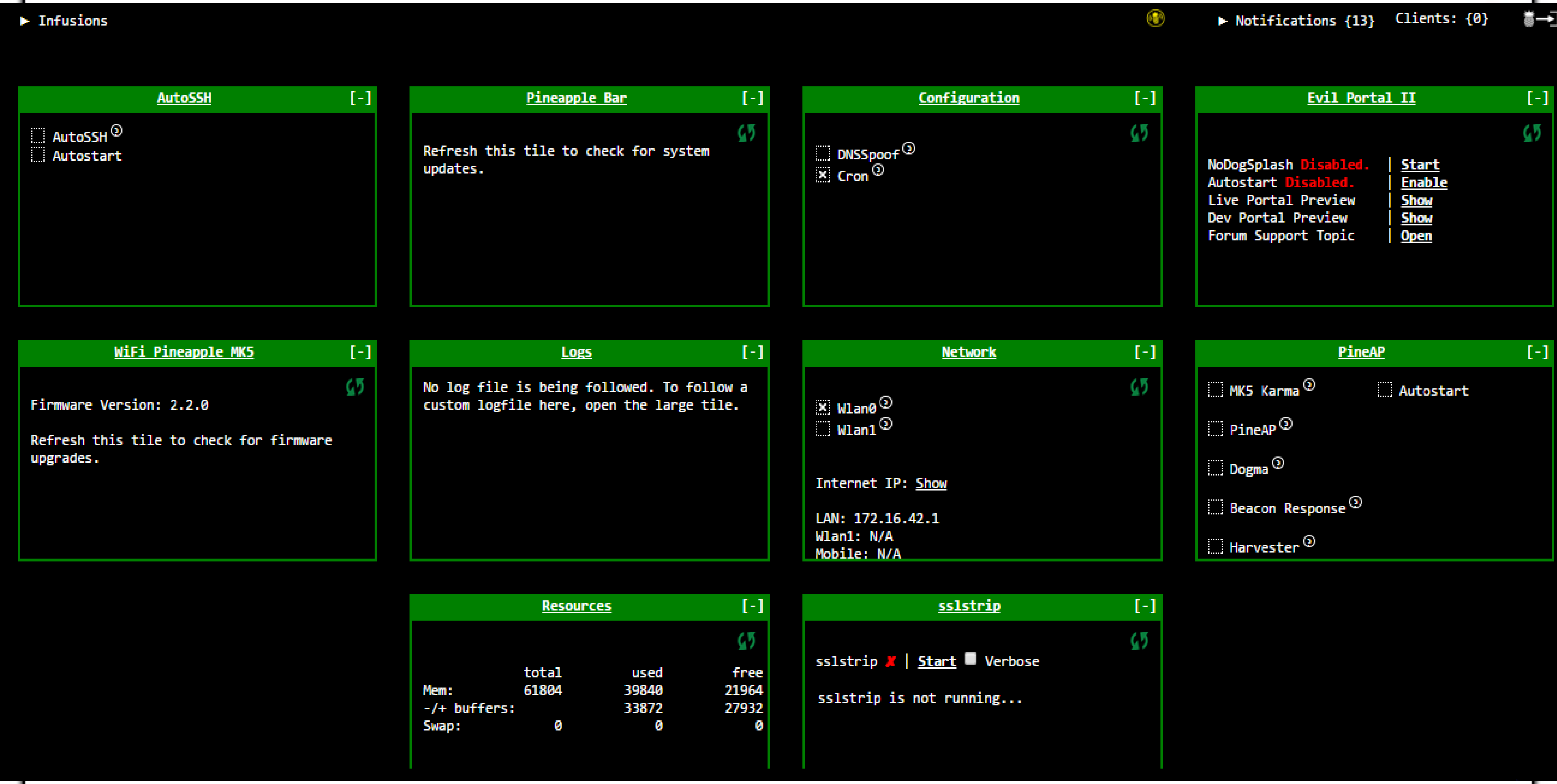








What does the Wi-Fi Pineapple do?



▶ Infusions ▶ Notifications {13} Clients: {0}

AutoSSH [-]

☐ AutoSSH
☐ Autostart

Pineapple Bar [-]

Refresh this tile to check for system updates.

Configuration [-]

☐ DNSSpoof
☒ Cron

Evil Portal II [-]

```
NoDogSplash Disabled.   | Start
Autostart Disabled.     | Enable
Live Portal Preview     | Show
Dev Portal Preview      | Show
Forum Support Topic     | Open
```

WiFi Pineapple MK5 [-]

Firmware Version: 2.2.0

Refresh this tile to check for firmware upgrades.

Logs [-]

No log file is being followed. To follow a custom logfile here, open the large tile.

Network [-]

☒ Wlan0
☐ Wlan1

Internet IP: Show

LAN: 172.16.42.1
Wlan1: N/A
Mobile: N/A

PineAP [-]

☐ MK5 Karma ☐ Autostart

☐ PineAP

☐ Dogma

☐ Beacon Response

☐ Harvester

Resources [-]

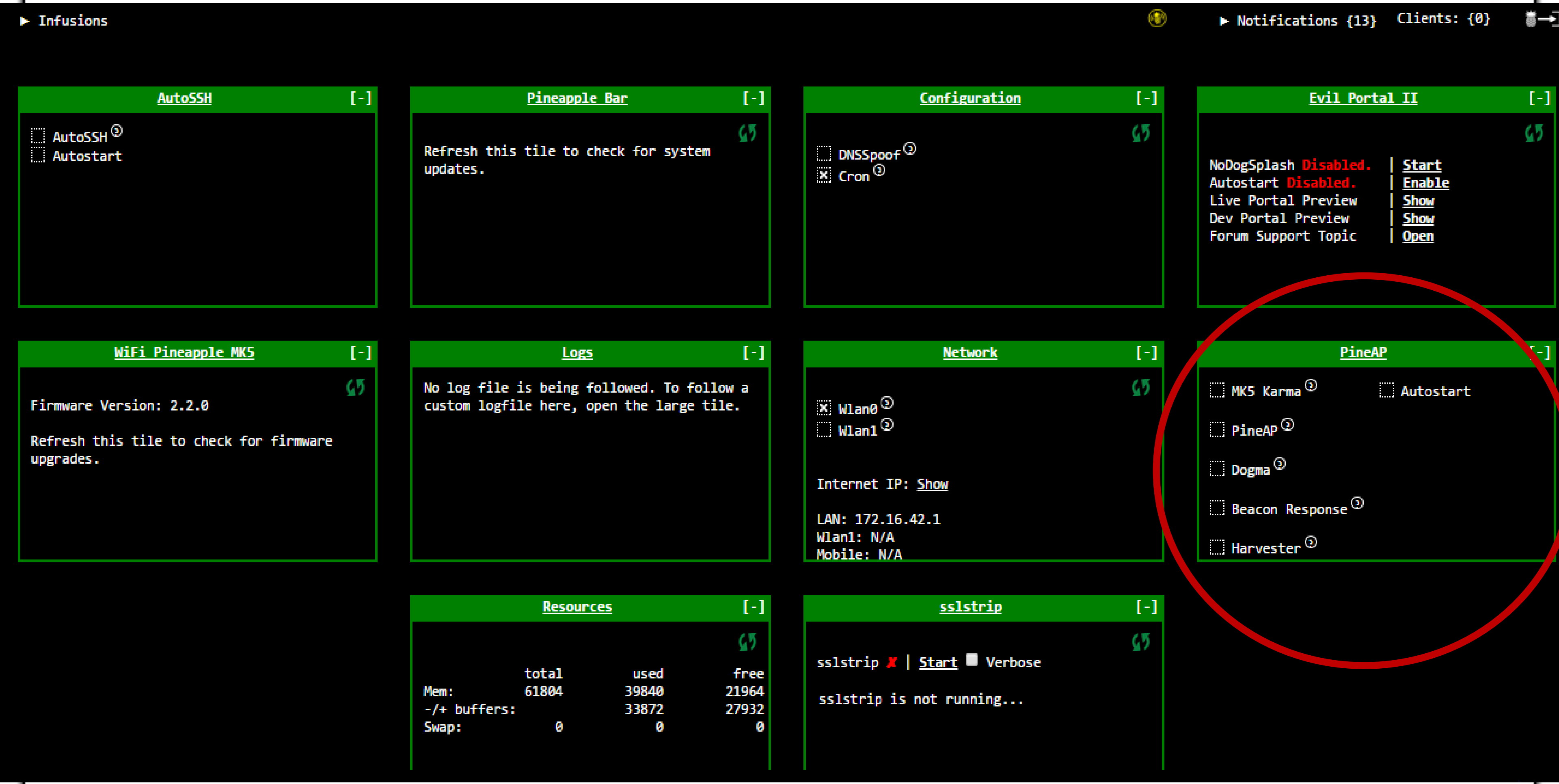
```
                 total       used       free
Mem:             61804      39840      21964
-/+ buffers:                33872      27932
Swap:                0          0          0
```

sslstrip [-]

sslstrip ✗ | Start ☐ Verbose

sslstrip is not running...

What does the Wi-Fi Pineapple do?



AutoSSH [-]

□ AutoSSH
□ Autostart

Pineapple Bar [-]

Refresh this tile to check for system updates.

Configuration [-]

□ DNSSpoof
☒ Cron

Evil Portal II [-]

```
NoDogSplash Disabled.   | Start
Autostart Disabled.     | Enable
Live Portal Preview     | Show
Dev Portal Preview      | Show
Forum Support Topic     | Open
```

WiFi Pineapple MK5 [-]

Firmware Version: 2.2.0

Refresh this tile to check for firmware upgrades.

Logs [-]

No log file is being followed. To follow a custom logfile here, open the large tile.

Network [-]

☒ Wlan0
□ Wlan1

Internet IP: Show

LAN: 172.16.42.1
Wlan1: N/A
Mobile: N/A

PineAP [-]

□ MK5 Karma   □ Autostart
□ PineAP
□ Dogma
□ Beacon Response
□ Harvester

Resources [-]

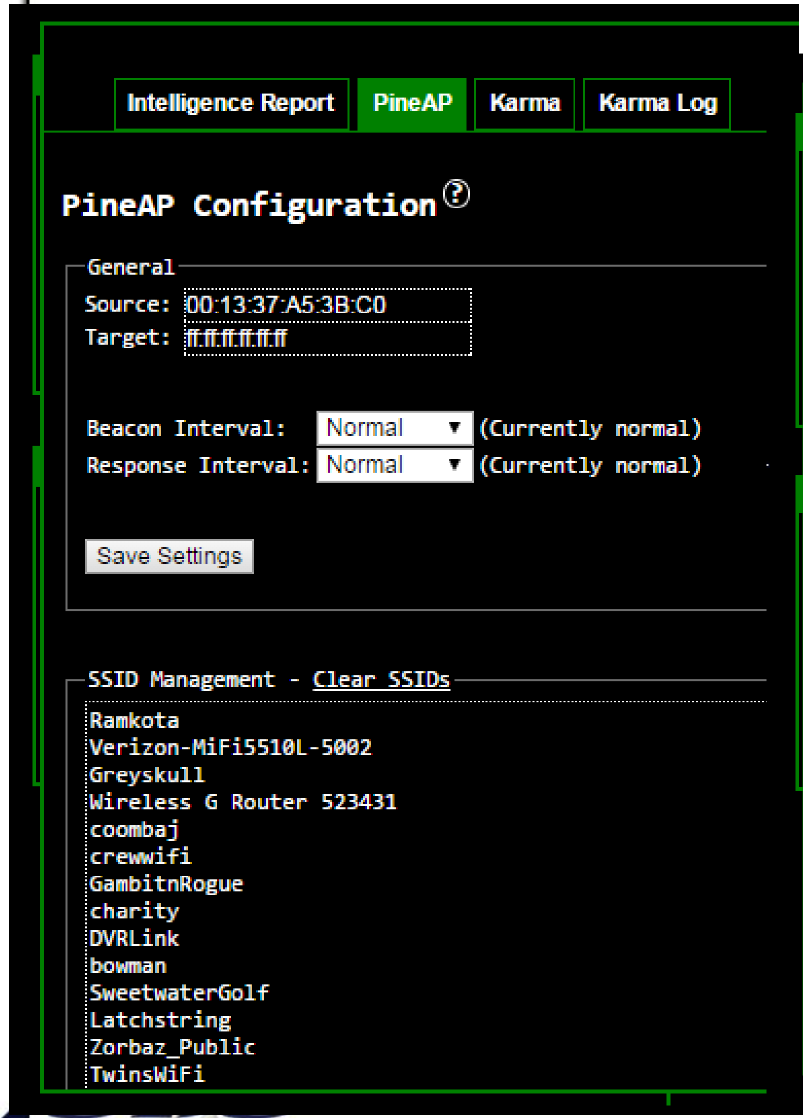
```
              total       used       free
Mem:          61804      39840      21964
-/+ buffers:             33872      27932
Swap:             0          0          0
```

sslstrip [-]

sslstrip ✗ | Start □ Verbose

sslstrip is not running...

What does the Wi-Fi Pineapple do?



PineAP Configuration

General

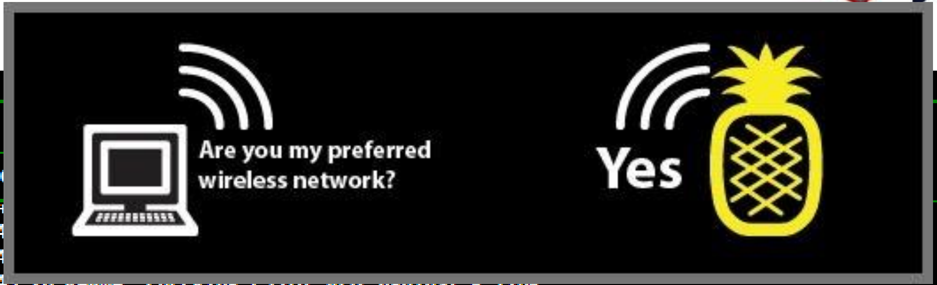
Source: 00:13:37:A5:3B:C0
Target: ff:ff:ff:ff:ff:ff

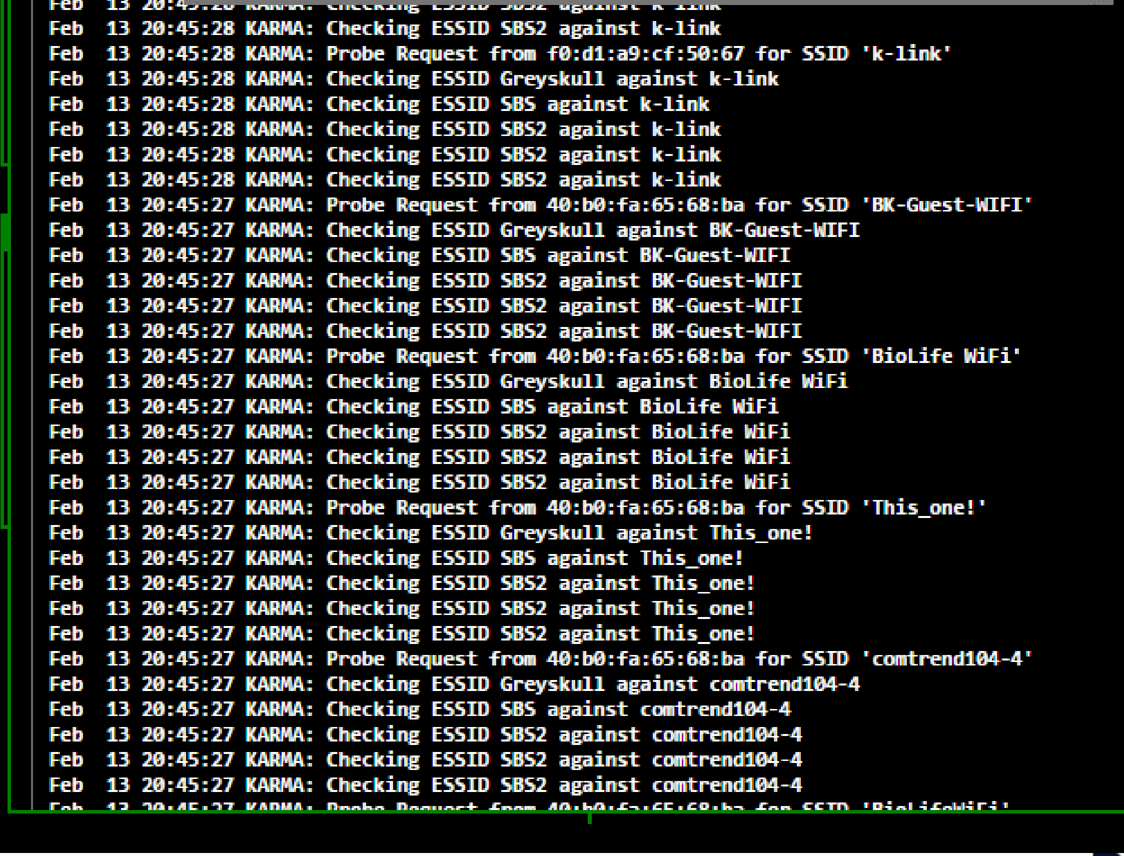
Beacon Interval: Normal (Currently normal)
Response Interval: Normal (Currently normal)

Save Settings

SSID Management - Clear SSIDs

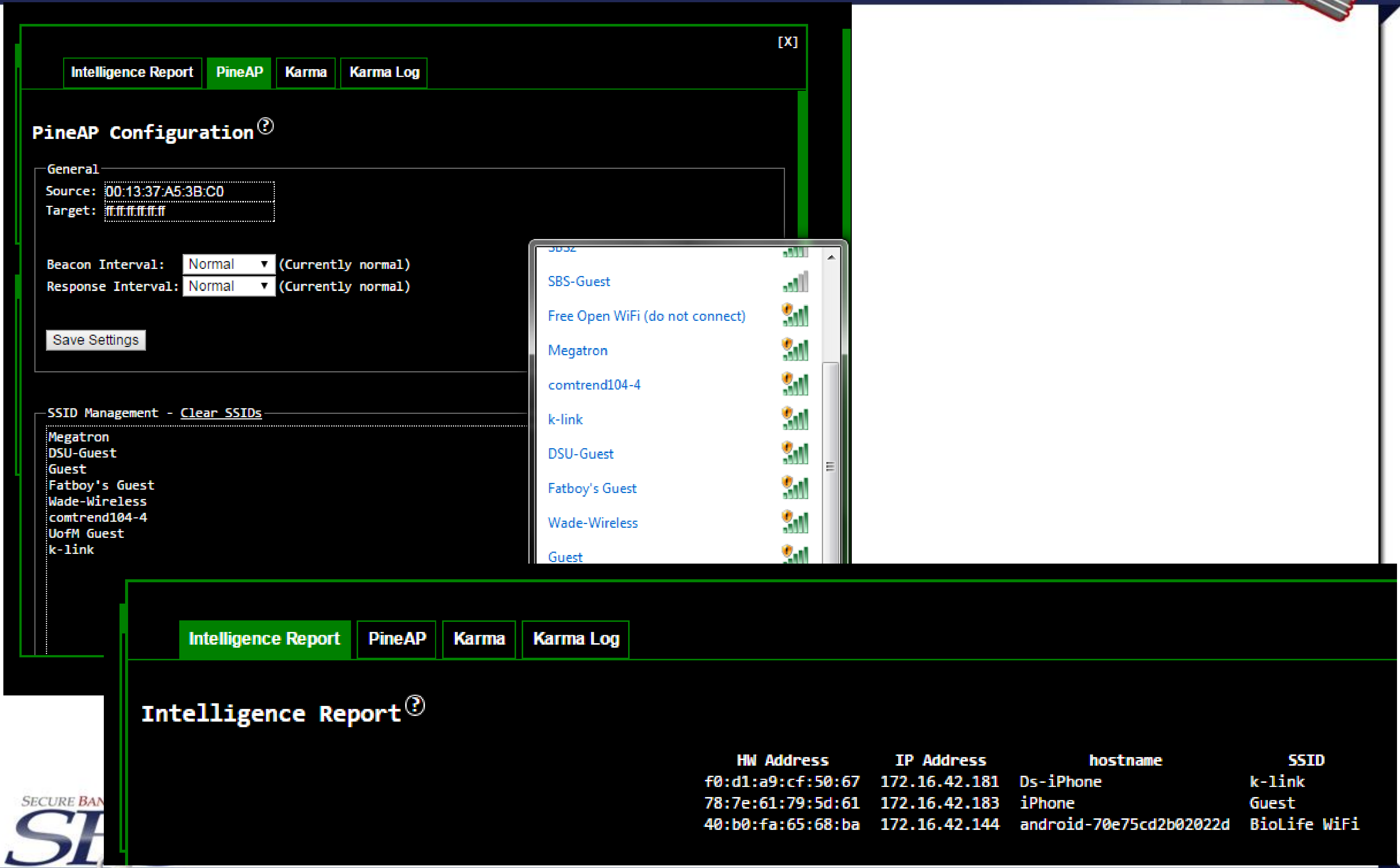
```
Ramkota
Verizon-MiFi5510L-5002
Greyskull
Wireless G Router 523431
coombaj
crewwifi
GambitnRogue
charity
DVRLink
bowman
SweetwaterGolf
Latchstring
Zorbaz_Public
TwinsWiFi
```





```
Feb  13 20:4
Feb  13 20:4
Feb  13 20:4
Feb  13 20:45:28 KARMA: Checking ESSID SBS2 against k-link
Feb  13 20:45:28 KARMA: Probe Request from f0:d1:a9:cf:50:67 for SSID 'k-link'
Feb  13 20:45:28 KARMA: Checking ESSID Greyskull against k-link
Feb  13 20:45:28 KARMA: Checking ESSID SBS against k-link
Feb  13 20:45:28 KARMA: Checking ESSID SBS2 against k-link
Feb  13 20:45:28 KARMA: Checking ESSID SBS2 against k-link
Feb  13 20:45:28 KARMA: Checking ESSID SBS2 against k-link
Feb  13 20:45:27 KARMA: Probe Request from 40:b0:fa:65:68:ba for SSID 'BK-Guest-WIFI'
Feb  13 20:45:27 KARMA: Checking ESSID Greyskull against BK-Guest-WIFI
Feb  13 20:45:27 KARMA: Checking ESSID SBS against BK-Guest-WIFI
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against BK-Guest-WIFI
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against BK-Guest-WIFI
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against BK-Guest-WIFI
Feb  13 20:45:27 KARMA: Probe Request from 40:b0:fa:65:68:ba for SSID 'BioLife WiFi'
Feb  13 20:45:27 KARMA: Checking ESSID Greyskull against BioLife WiFi
Feb  13 20:45:27 KARMA: Checking ESSID SBS against BioLife WiFi
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against BioLife WiFi
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against BioLife WiFi
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against BioLife WiFi
Feb  13 20:45:27 KARMA: Probe Request from 40:b0:fa:65:68:ba for SSID 'This_one!'
Feb  13 20:45:27 KARMA: Checking ESSID Greyskull against This_one!
Feb  13 20:45:27 KARMA: Checking ESSID SBS against This_one!
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against This_one!
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against This_one!
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against This_one!
Feb  13 20:45:27 KARMA: Probe Request from 40:b0:fa:65:68:ba for SSID 'comtrend104-4'
Feb  13 20:45:27 KARMA: Checking ESSID Greyskull against comtrend104-4
Feb  13 20:45:27 KARMA: Checking ESSID SBS against comtrend104-4
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against comtrend104-4
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against comtrend104-4
Feb  13 20:45:27 KARMA: Checking ESSID SBS2 against comtrend104-4
Feb  13 20:45:27 KARMA: Probe Request from 40:b0:fa:65:68:ba for SSID 'BioLifeWiFi'
```

The results…



PineAP Configuration

General
Source: 00:13:37:A5:3B:C0
Target: ff:ff:ff:ff:ff:ff

Beacon Interval: Normal (Currently normal)
Response Interval: Normal (Currently normal)

SSID Management - Clear SSIDs

```
Megatron
DSU-Guest
Guest
Fatboy's Guest
Wade-Wireless
comtrend104-4
UofM Guest
k-link
```

SBS-Guest
Free Open WiFi (do not connect)
Megatron
comtrend104-4
k-link
DSU-Guest
Fatboy's Guest
Wade-Wireless
Guest

Intelligence Report

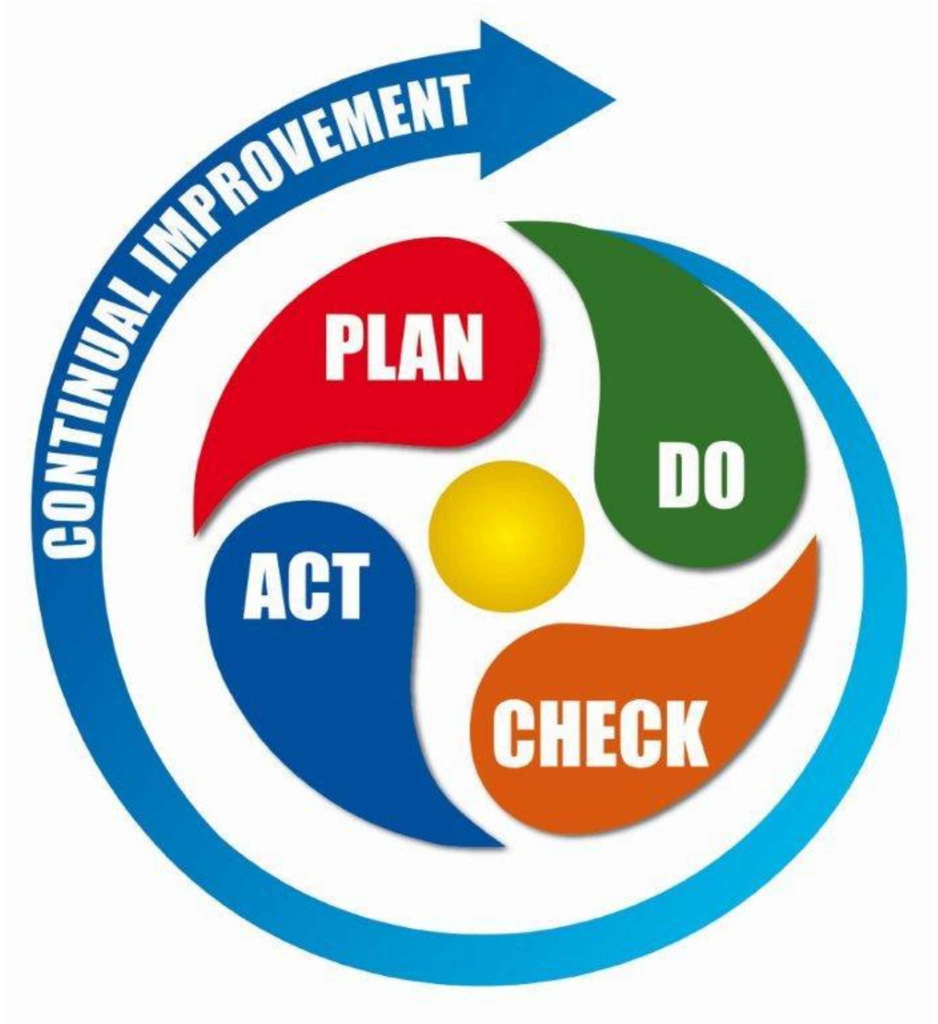
```
    HW Address        IP Address          hostname              SSID
f0:d1:a9:cf:50:67   172.16.42.181   Ds-iPhone                 k-link
78:7e:61:79:5d:61   172.16.42.183   iPhone                    Guest
40:b0:fa:65:68:ba   172.16.42.144   android-70e75cd2b02022d   BioLife WiFi
```

How to manage these risks?

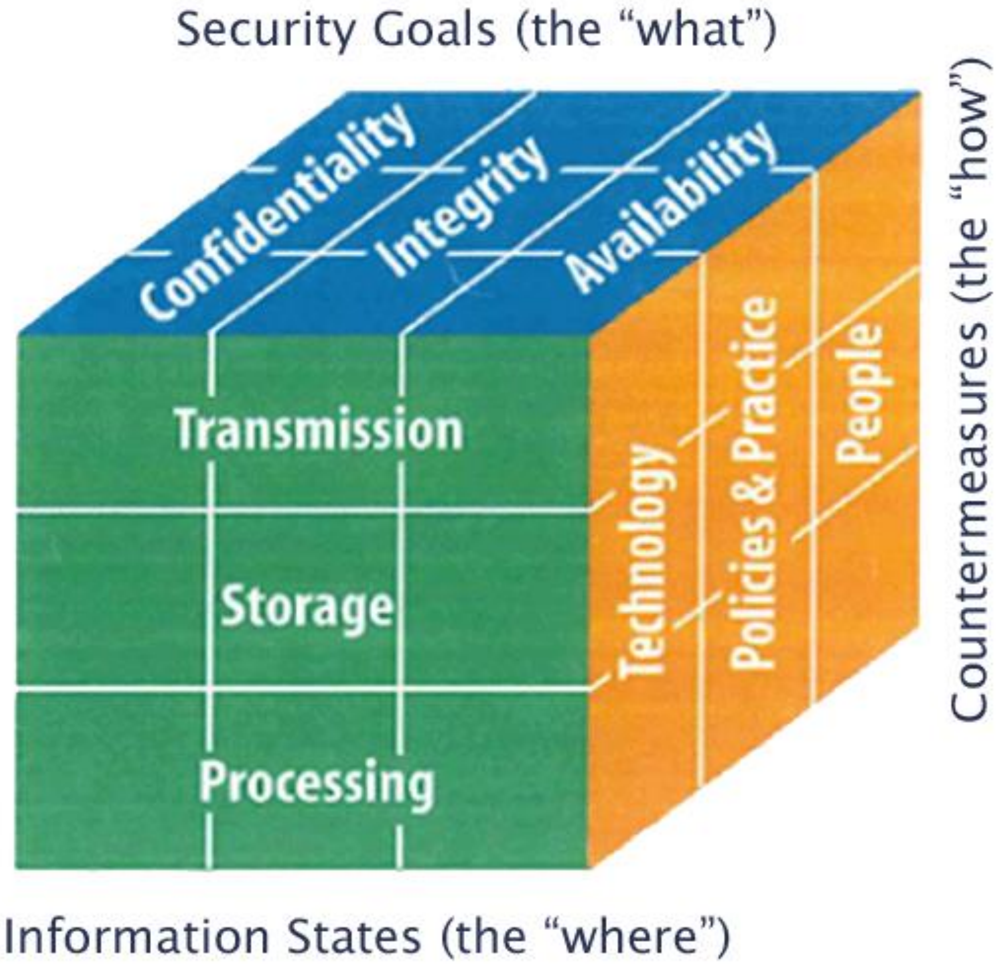
- How should you manage the risk to your institution on a go-forward basis?

Answers!

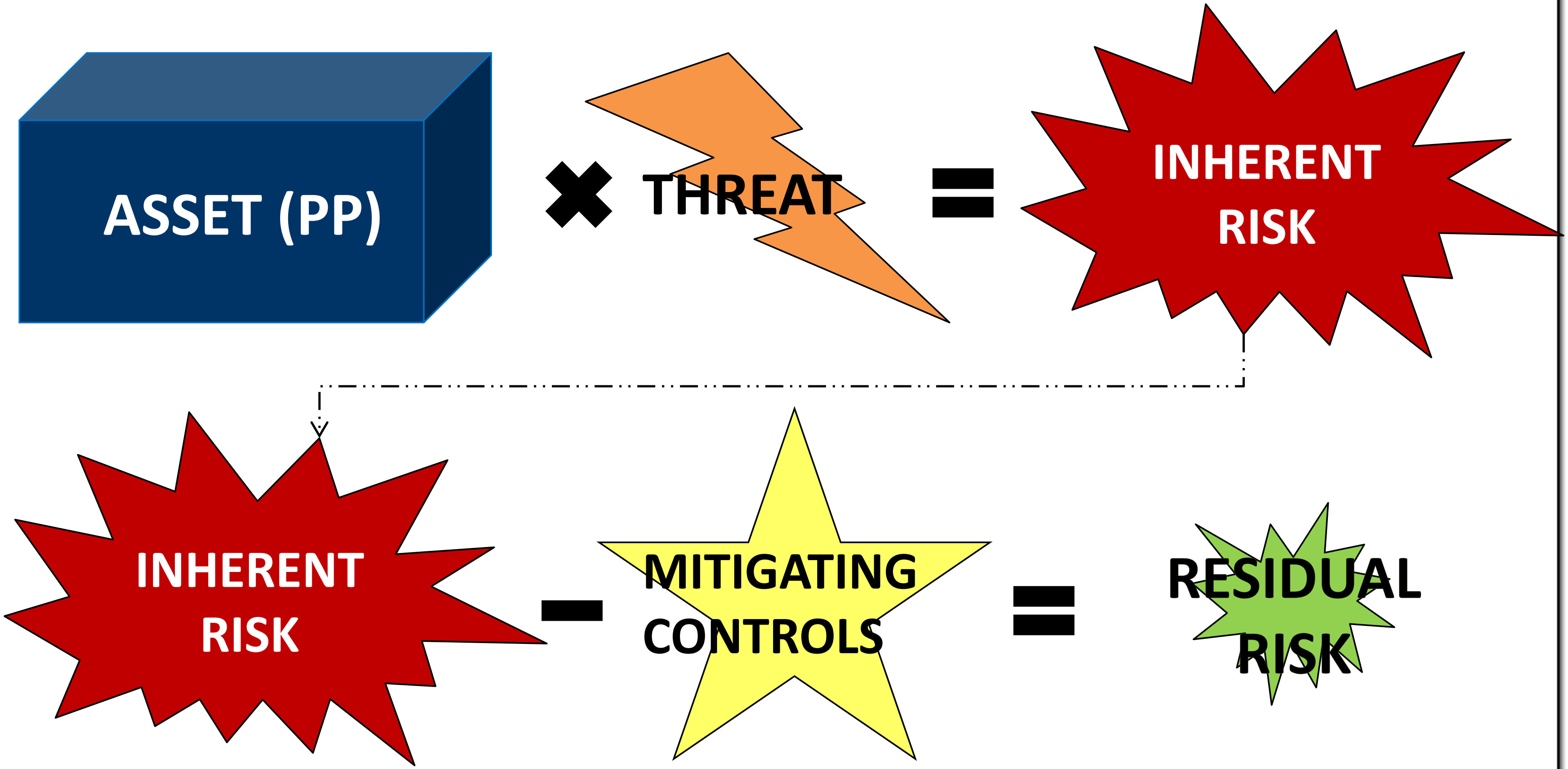
- **Plan**
  - Assess your risk
  - No, REALLY assess it
- **Do**
  - Build your ISP
  - Implement controls
- **Check**
  - Test your people
  - Test your process
  - Test your technology
- **Act**
  - Apply lessons learned
  - Continuously improve!



The McCumber Cube!



How does Risk Assessment work?



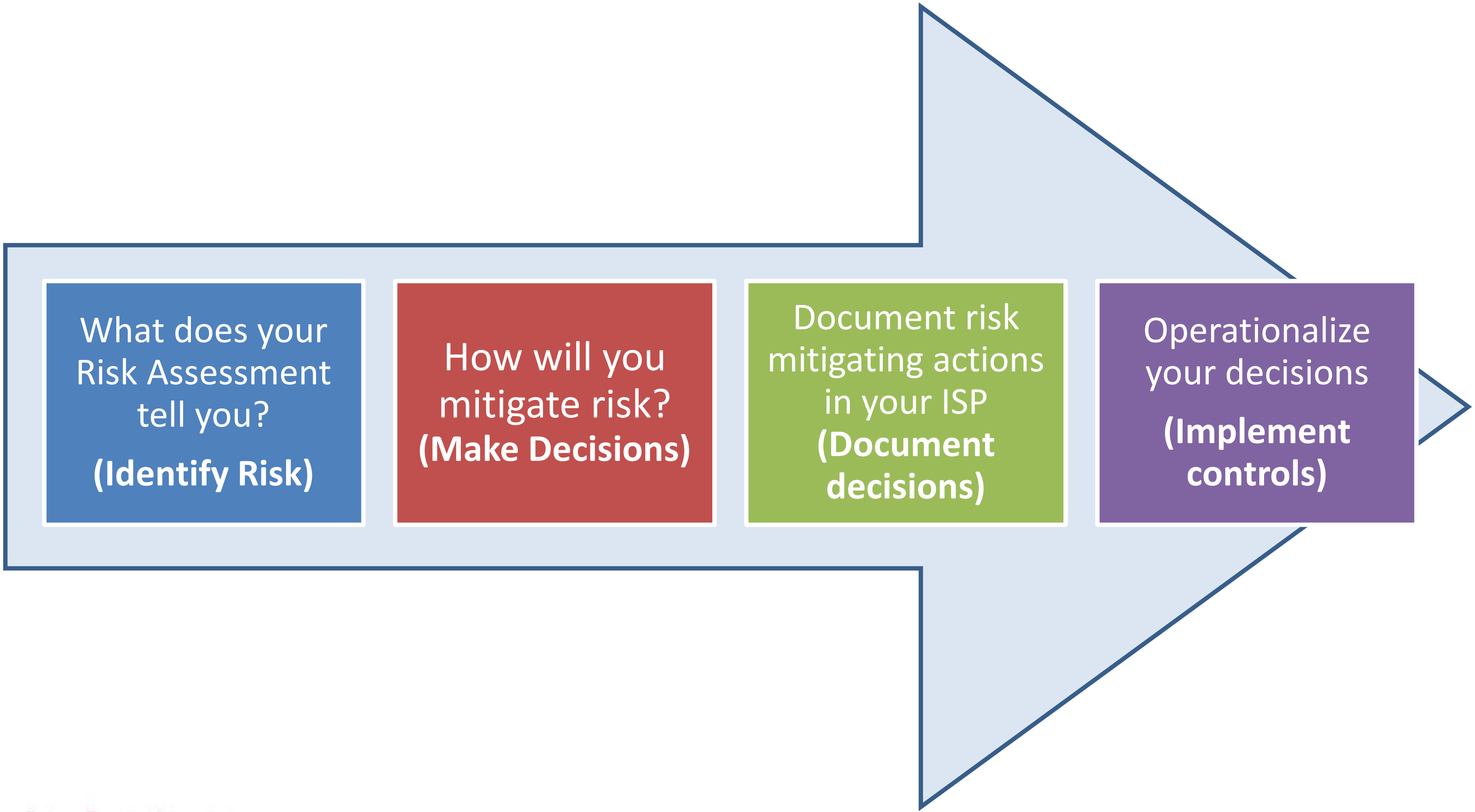
ASSET (PP) ✖ THREAT = INHERENT RISK

INHERENT RISK – MITIGATING CONTROLS = RESIDUAL RISK

Keys to assessing your Risk (Plan!)

- Get rid of your subjectivity… it's time to QUANTIFY your risk
- If you can't quantify your risk, how can you measure it? How can you improve?
- Set goals!
- Know your Acceptable Levels of Risk
- Not just IT Assets, but for other areas
  - Business processes
  - Vendors
  - Enterprise Risk

Build your ISP (Do!)



What does your Risk Assessment tell you?

(Identify Risk)

How will you mitigate risk?

(Make Decisions)

Document risk mitigating actions in your ISP

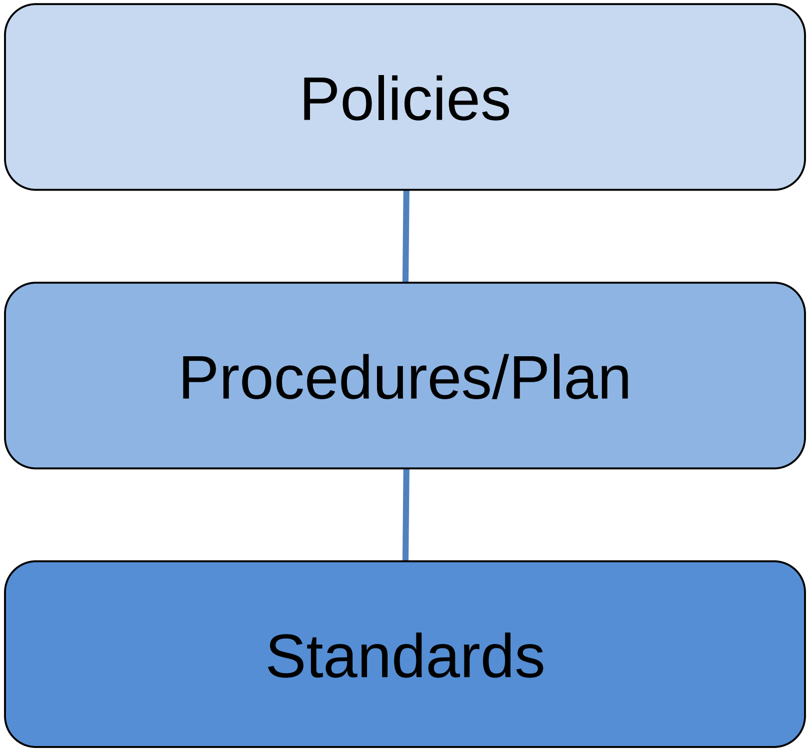
(Document decisions)

Operationalize your decisions

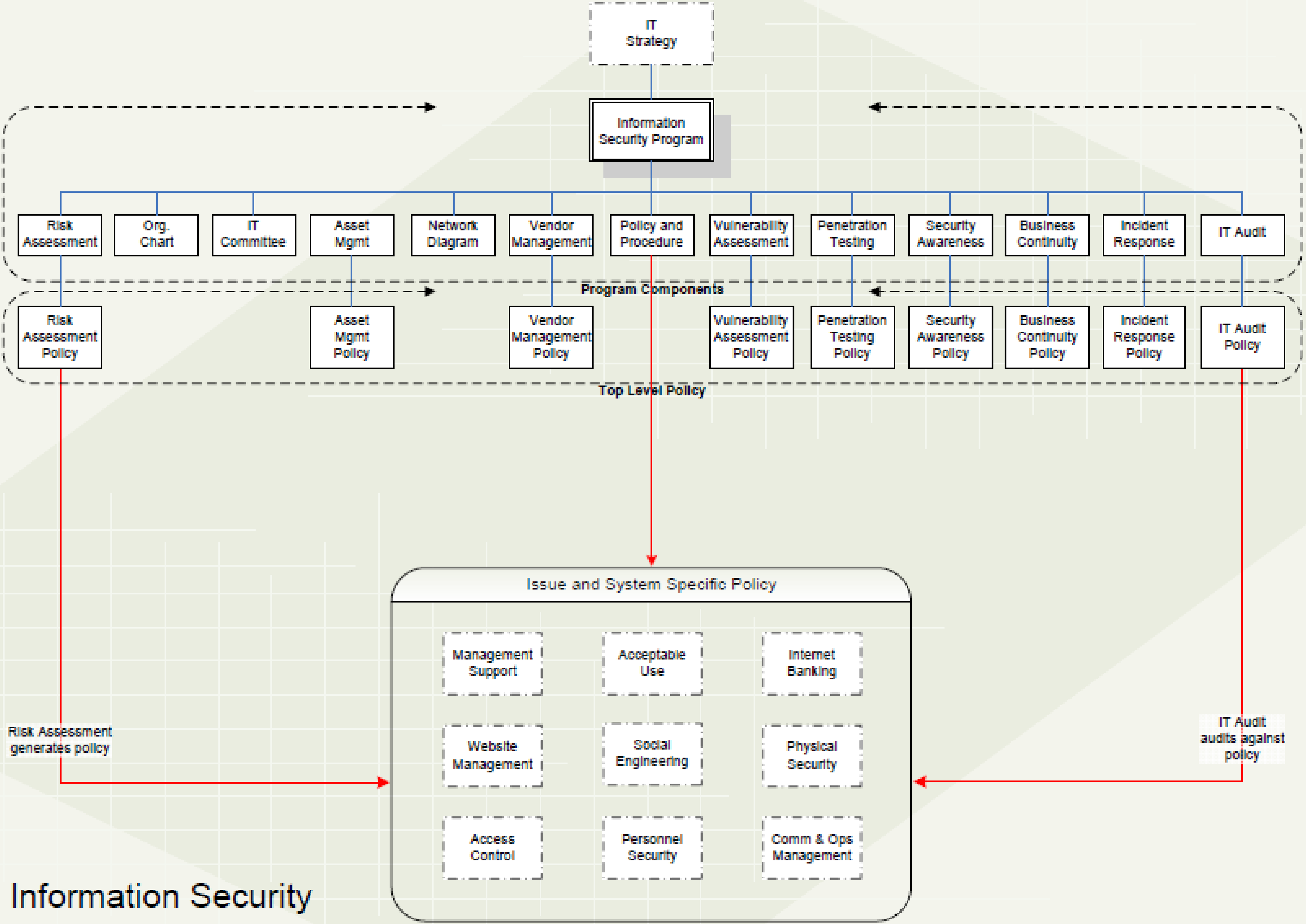
(Implement controls)

ISP for Community Banks

- Information Security Program Blueprint
  - I.T. Risk Assessment
  - Asset Management
  - Vendor Management
  - Penetration Testing
  - Vulnerability Assessment
  - Security Awareness
  - Business Continuity
  - Incident Response
  - I.T. Audit



Support Structures
- Organizational Chart
- I.T. Committee
- Network Diagram



IT Strategy

Information Security Program

Risk Assessment

Org. Chart

IT Committee

Asset Mgmt

Network Diagram

Vendor Management

Policy and Procedure

Vulnerability Assessment

Penetration Testing

Security Awareness

Business Continuity

Incident Response

IT Audit

Program Components

Risk Assessment Policy

Asset Mgmt Policy

Vendor Management Policy

Vulnerability Assessment Policy

Penetration Testing Policy

Security Awareness Policy

Business Continuity Policy

Incident Response Policy

IT Audit Policy

Top Level Policy

Issue and System Specific Policy

Management Support

Acceptable Use

Internet Banking

Website Management

Social Engineering

Physical Security

Access Control

Personnel Security

Comm & Ops Management

Risk Assessment generates policy

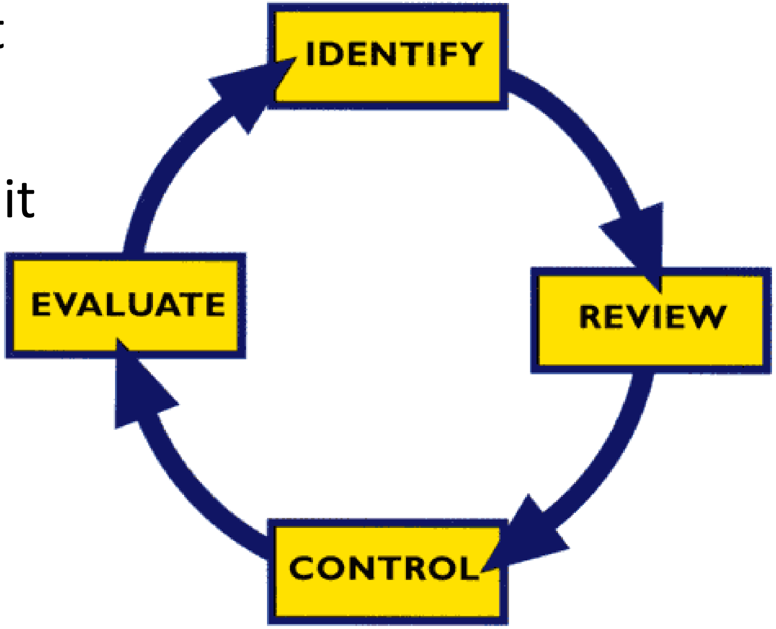
IT Audit audits against policy

Information Security Program - Flow

Version: 1.04

Test your Program (Check!)

1. Assess Risk
2. Implement Controls
3. Audit Controls
   - People
     - Social Engineering Assessment
   - Process
     - Info Technology / Security Audit
   - Technology
     - Vulnerability Assessment
     - Penetration Testing



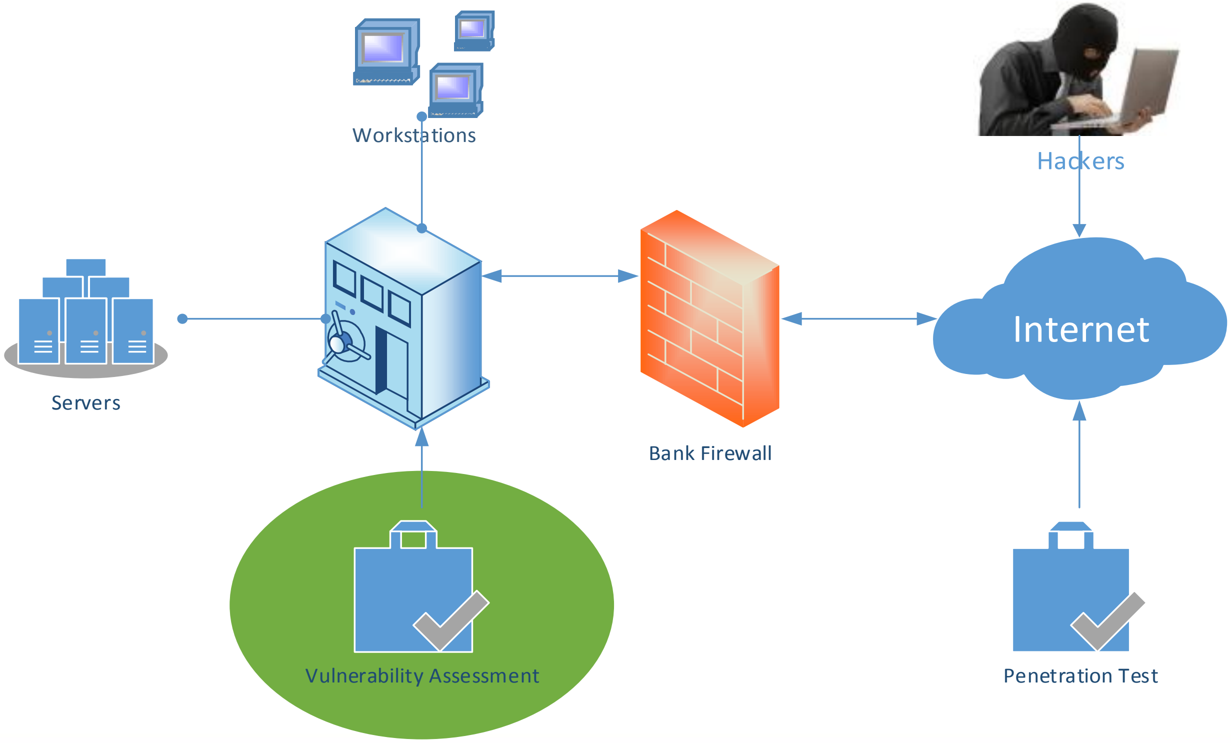
Info Technology / Security Audit

- Check your overall security program
- Identify other risk you may not have considered
- Outline basic components specific to your business
- Highlight best practices

I'll need to see some process documentation for what you're doing there.
I was just sharpening this pencil!
Oh...then I'll need training and safety procedures, too.

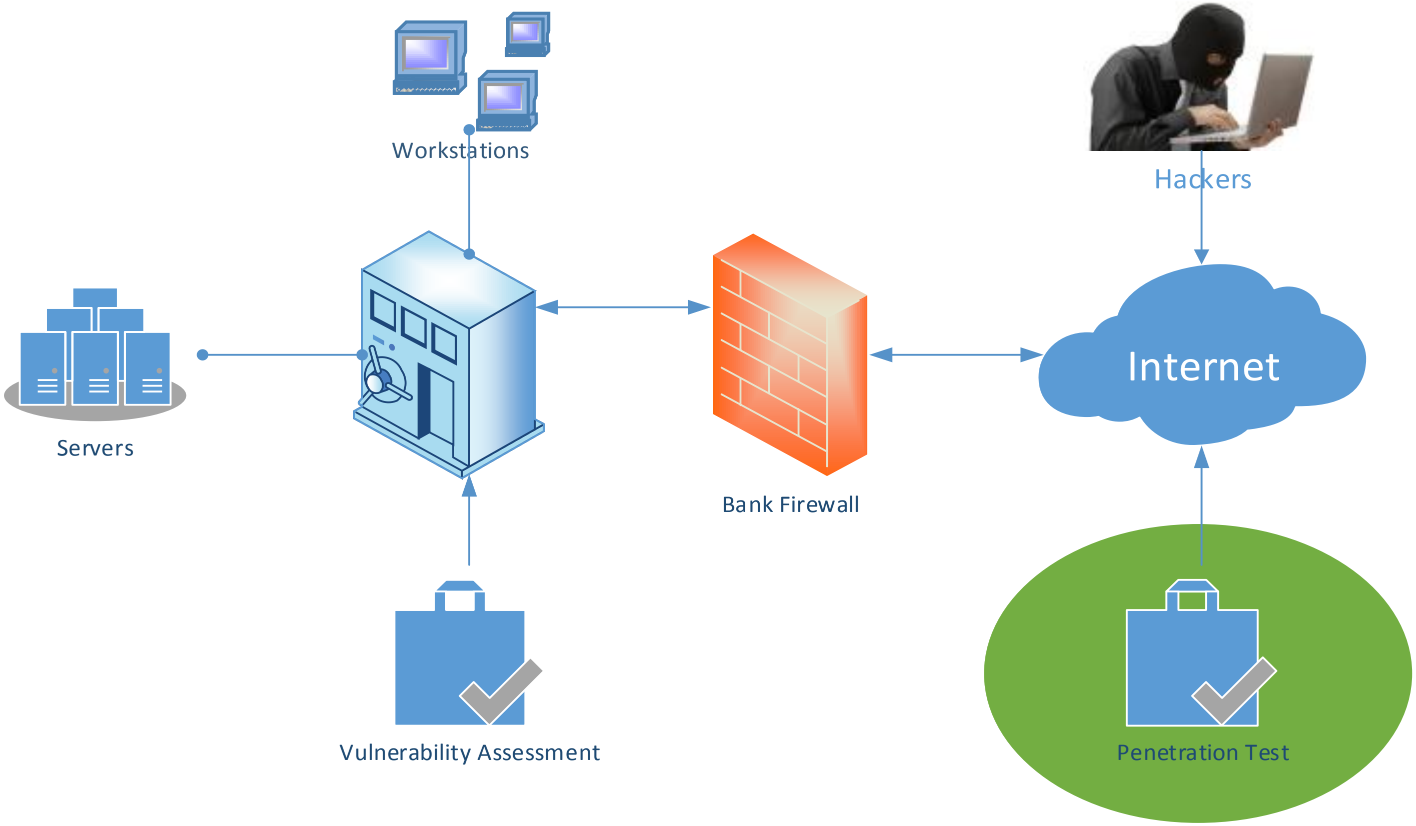
Vulnerability Assessment

- Check Software Patching
- Check Malware
- Check Default Security Settings



Penetration test

- Replicates a Hackers Actions to Break-in
- Check Hardware Firewall



Social Engineering

- Test your people
- Check effectiveness of training program
- Types Include:
  - Phishing Emails
  - Phone Impersonation
  - Physical Impersonation
  - Dumpster Diving

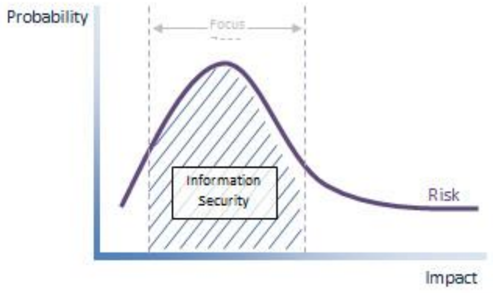
SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.

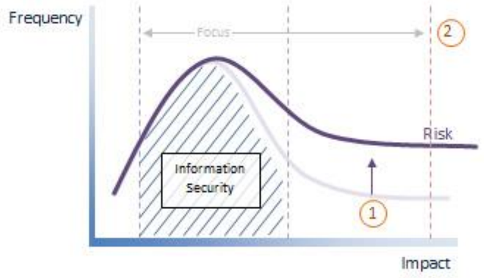
Social Engineering

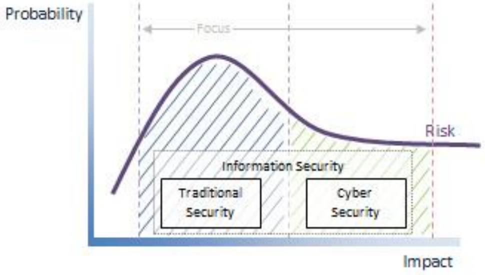
DISCOVERY
Sometimes, the greatest treasures are found beneath piles of trash.

What is “Cybersecurity”?

- **Cyber Risk**
  - the increased probability that the very-high-impact, internet-based risks and threats we once thought were improbably will harm our networks
- **Cybersecurity**
  - the controls and processes in place to protect our networks and customer information from cyber risk
- **How does it relate to Information Security?**
  - discipline of Information Security, which not only encompasses Cybersecurity, but also all of the traditional things we’ve done to protect our confidential customer information, including IT Risk Assessment, Vendor Management, Business Continuity Planning, Vulnerability Assessment, IT Audit, and much more







Images courtesy of ISACA and member Menny Barzilay
http://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=296

What's up with Cybersecurity Assessments?

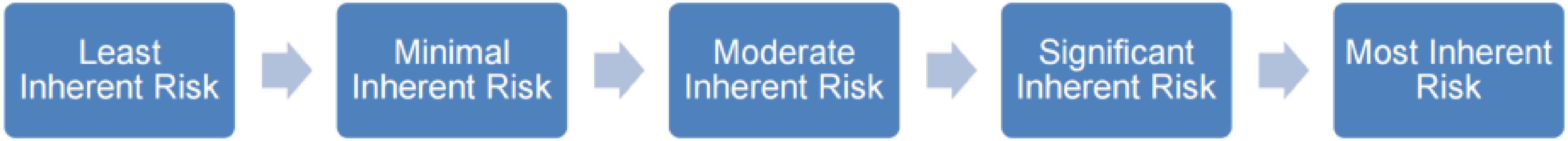
- FFIEC Cybersecurity Assessment Tool released on Tuesday June 30th, 2015
- Not really a "tool," as we have traditionally defined software or hardware
- More of a process to help banks perform a self-assessment on their Cybersecurity Preparedness
- Based on size-and-complexity
- Resulting from the 2014 Cybersecurity Assessment lessons-learned

FFIEC CA Tool (3 parts)

- Three (3) major components
  1. Rating your **Inherent Risk** for Cybersecurity threats based on your size and complexity
  2. Rating your **Cybersecurity Maturity** regarding how prepared you are to handle different Cybersecurity threats
  3. **Interpreting and analyzing** your results by understanding how your Inherent Risk ties to your Cybersecurity Maturity, and where you SHOULD be regarding risk vs. maturity.

Cybersecurity Inherent Risk

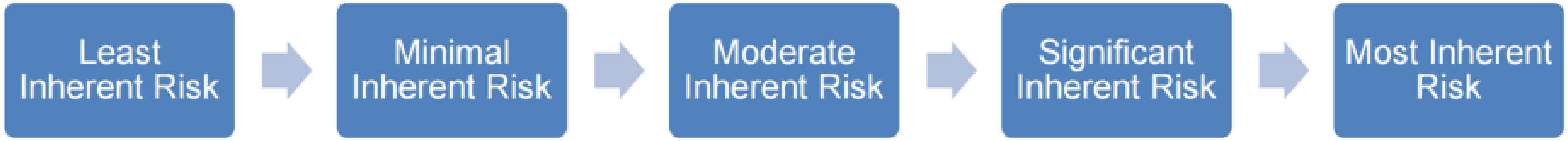
- Very PRESCRIPTIVE
- Really getting to the Size and Complexity issue originally stated by GLBA
- Allows organizations to determine how much Inherent Risk (before controls) their institution faces regarding these new Cybersecurity threats



Least Inherent Risk → Minimal Inherent Risk → Moderate Inherent Risk → Significant Inherent Risk → Most Inherent Risk

Cybersecurity Inherent Risk

- Five Inherent Risk Areas
  1. Technologies and Connection Types
  2. Delivery Channels
  3. Online/Mobile Products and Technology Services
  4. Organizational Characteristics
  5. External Threats



Least Inherent Risk → Minimal Inherent Risk → Moderate Inherent Risk → Significant Inherent Risk → Most Inherent Risk

Cybersecurity Maturity

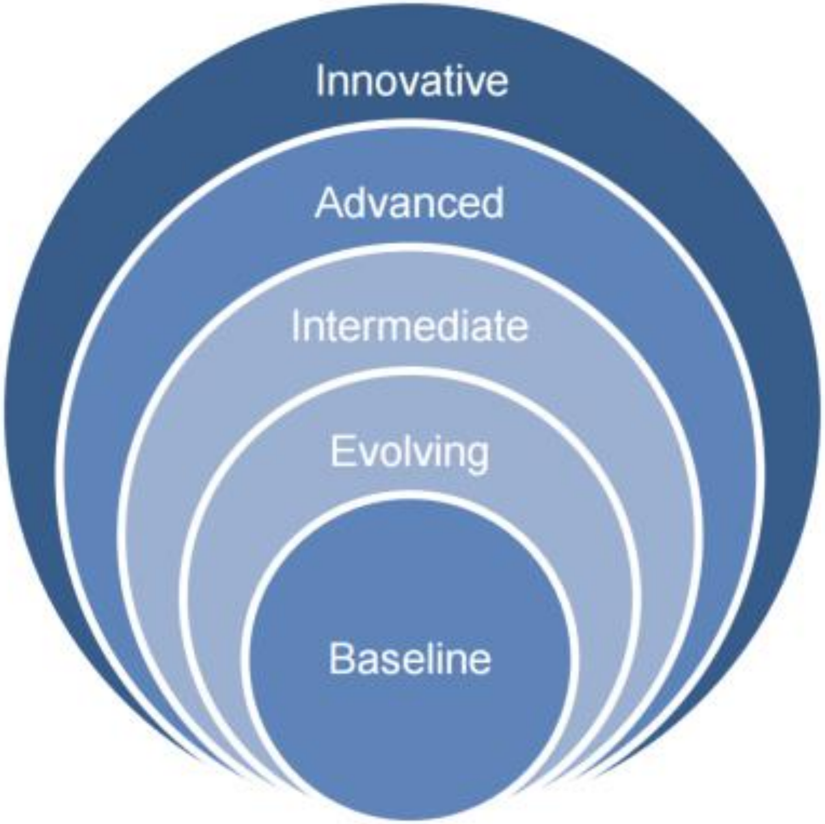
Measure Maturity in 5 Domains (+ Assessment Factors)

1. Cyber Risk Management and Oversight
   - Governance, Risk Management, Resources, and Training
2. Threat Intelligence and Collaboration
   - Threat Intelligence, Monitoring & Analyzing, and Info Sharing
3. Cybersecurity Controls
   - Preventative, Detective, and Corrective controls
4. External Dependency Management
   - External Connections and (Vendor) Relationship Management
5. Cyber Incident Management and Resilience
   - Incident Resilience Planning, Detection, Response, & Mitigation, and Escalation & Reporting

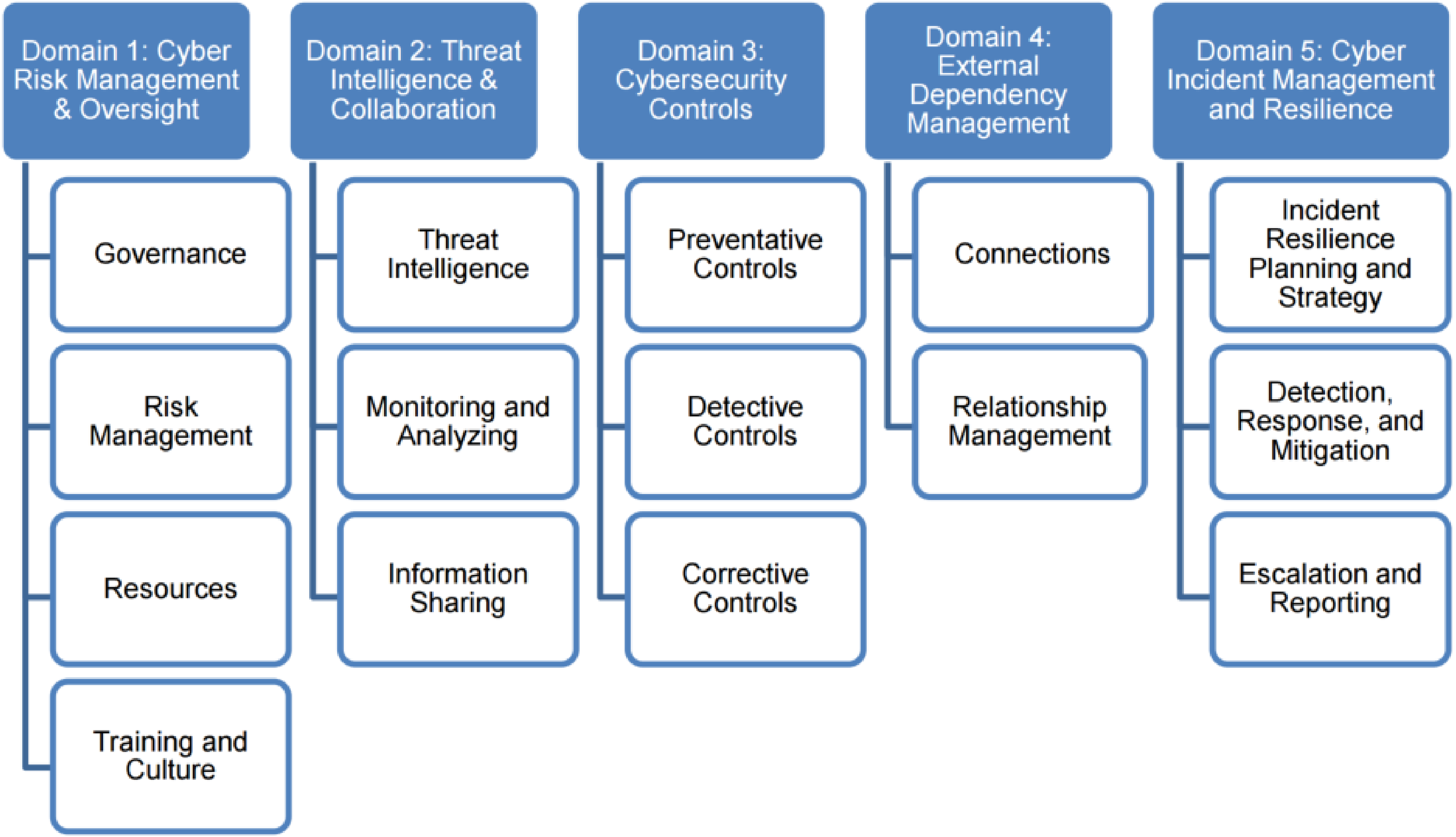
How does Cybersecurity Maturity work?

Measured by 5 Cybersecurity Maturity Levels

1. Baseline
2. Evolving
3. Intermediate
4. Advanced
5. Innovative



Domains and Assessment Factors



Domain 1: Cyber Risk Management & Oversight

- Governance
- Risk Management
- Resources
- Training and Culture

Domain 2: Threat Intelligence & Collaboration

- Threat Intelligence
- Monitoring and Analyzing
- Information Sharing

Domain 3: Cybersecurity Controls

- Preventative Controls
- Detective Controls
- Corrective Controls

Domain 4: External Dependency Management

- Connections
- Relationship Management

Domain 5: Cyber Incident Management and Resilience

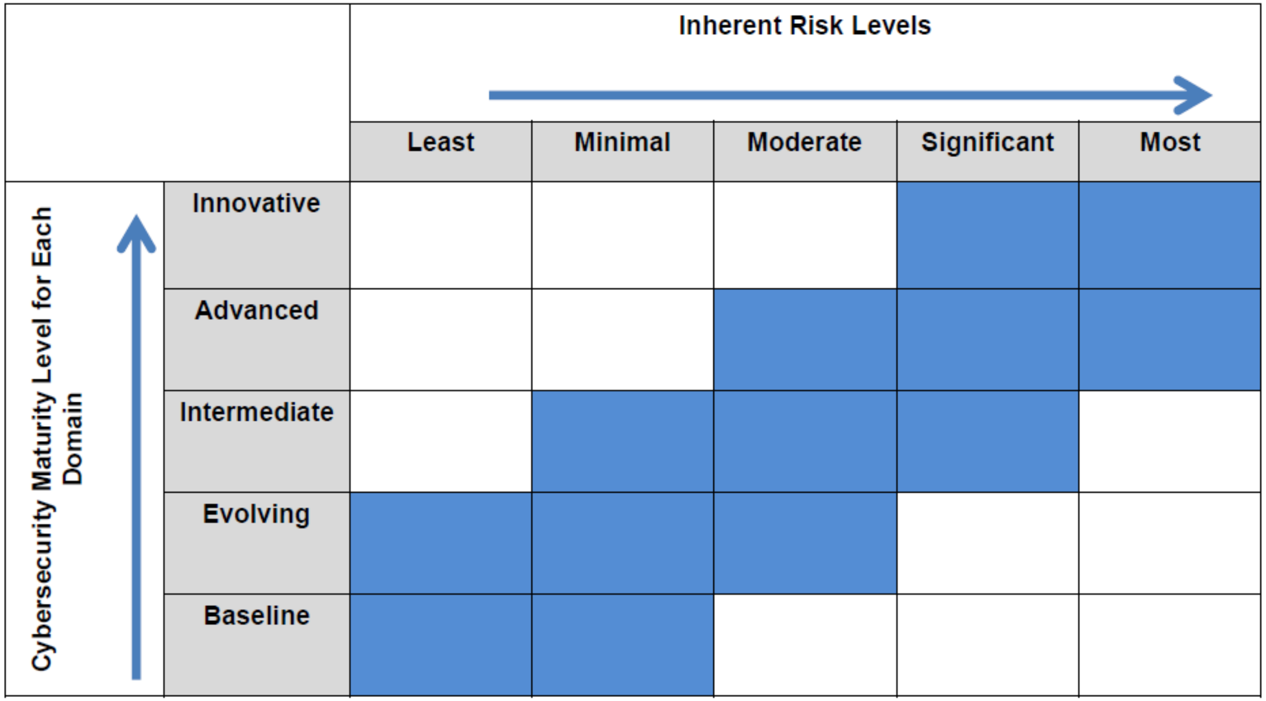
- Incident Resilience Planning and Strategy
- Detection, Response, and Mitigation
- Escalation and Reporting

Inherent Risk vs. Maturity

- All good Risk Management processes help make decisions and set goals
- How does one determine Inherent Risk versus Cybersecurity Maturity?
- And more importantly, what is the right Inherent Risk vs. Maturity level?

Increasing Maturity

Table 3: Risk/Maturity Relationship



		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				🟦	🟦
	Advanced			🟦	🟦	🟦
	Intermediate		🟦	🟦	🟦	
	Evolving	🟦	🟦	🟦		
	Baseline	🟦	🟦			

Domain 1: Cyber Risk Management and Oversight

Domain 2: Threat Intelligence and Collaboration

Domain 3: Cybersecurity Controls

Domain 4: External Dependency Management

Domain 5: Cyber Incident Management and Resilience

SBS FREE Cyber-RISK Tool

- Goals of the FREE Cyber-RISK^{tm} tool:
  1. Automate the Cybersecurity Assessment Tool
  2. Save you from creating your own spreadsheet
  3. Make your life easier and more efficient
  4. Provide you with one-click reports
  5. Improve the process by tying the Inherent Risk and Cybersecurity Maturity processes together more intuitively
  6. Get you peer comparison data (down the road)
  7. Access to your own personal Information Security Expert if you need us!

Additional Cyber Security Resources

- SBS Cybersecurity Assessment Blog:
  - https://www.protectmybank.com/ffiec-cybersecurity-assessment-resources/
- Register for the Cyber-RISK tool:
  - https://cyber-risk.protectmybank.com/
- SBS Institute Certifications:
  - https://www.protectmybank.com/sbsinstitute/

That’s all she wrote…

- Any questions, comments, or concerns?
- Automate your IT Risk Assessment – TRAC!
- Also, for a much deeper dive on Information Security specifically for Community Banks, check out our new Community Bank Certification Programs!
  - CCB Vendor Manager (CCBVM)
  - CCB Security Professional (CCBSP)
  - CCB Technical Professional (CCBTP)
  - CCB Ethical Hacker (CCBEH)
  - CCB Incident Responder CCBIH)
  - Ask us about it!
- Contact info:
  - Jon Waldman, Partner
    - jon@protectmybank.com
    - 605-380-8897