Proactive Security: Effective Cyber Risk Mitigation

Dave Shackleford

Founder and Principal Consultant, Voodoo Security

Agenda

- This talk will really be split into two sections
- The first will focus on new ways of thinking about your security program
- The second will focus on ways that you can apply new strategies to be more effective

Change your mojo

Think like an entrepreneur & be more creative

Not your usual intro.

- I normally start these things with the “Blah Blah Blah we’re not winning Blah Blah Blah” speech.
- But you already knew that.
- Instead, let’s talk about insanity.

> "Insanity is doing the same thing over and over again but expecting different results."

It’s time to think like entrepreneurs.

- This may seem like a stretch.
- It’s not.
- There’s one fundamental change in your thinking you’ll need to make: “What is your product”?
- Along with that, you will need to package it, sell it, and improve it over time.
- Let’s examine four questions we need to answer.

Question #1: Do Consumers Recognize the Problem We Solve?

Things to Consider

- First, who are your consumers?
  - Executives
  - IT
  - Business Units
  - Partners
  - General employees

- Second, what problem do you solve?
  - For security, likely "Ongoing risk intelligence and mitigation for cyber risks".

Question #2: If there's a solution, will the consumers buy it?

Things to Consider

- There are lots of reasons the answer is “yes”
  - Compliance
  - Risk awareness
  - Peer/business pressure
  - Stakeholder pressure
- However, there are lots of reasons they WON’T.
  - Politics
  - $$$
  - You. Yes, YOU.

Question #3: Will consumers buy the solution **from us**?

Things to Consider

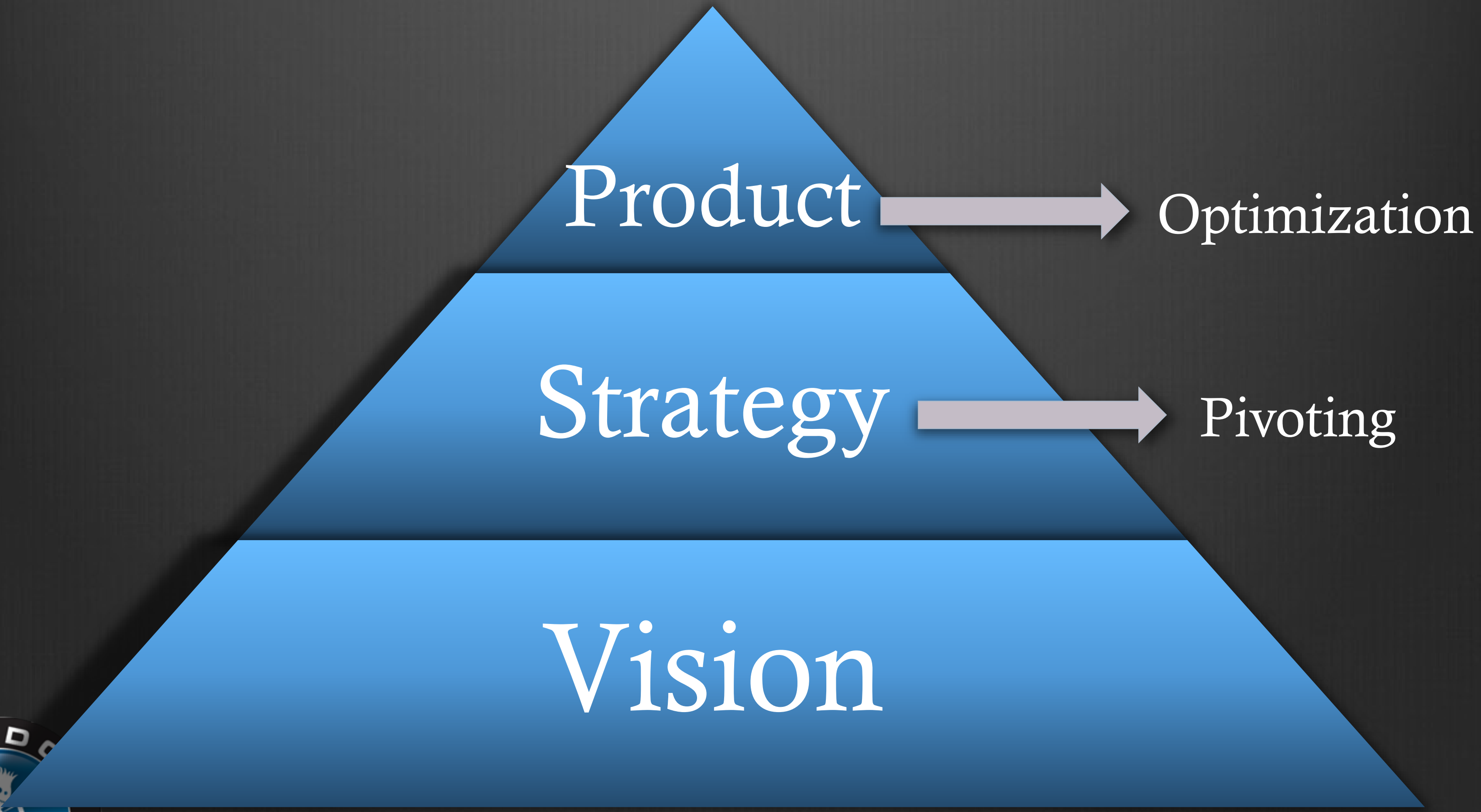
- You need your organization to buy your product, namely security intelligence and risk management services and capabilities.
- There are plenty of reasons why you may be having trouble with this.
  - Your selling ability.
  - Your demeanor.
  - Your security program.
  - Your people.
  - Things beyond your control.

Question #4: Can we build a solution for the problem?

Things to Consider

- You need your organization to buy your product, namely security intelligence and risk management services and capabilities.
- There are plenty of reasons why you may be having trouble with this.
  - Your selling ability.
  - Your demeanor.
  - Your security program.
  - Your people.
  - Things beyond your control.

The Entrepreneur Pyramid



Product → Optimization

Strategy → Pivoting

Vision

Thoughts for Security

Category	Security Considerations
Vision	1. Have a security mission statement! 2. Have definitive outcomes of your efforts tied to the vision.
Strategy	1. This is people, process, and technologies. 2. How will you accomplish the vision?
Product	1. This is the outcome of your strategy. 2. It should be **measurable**! 3. You should be focused primarily on the MVP

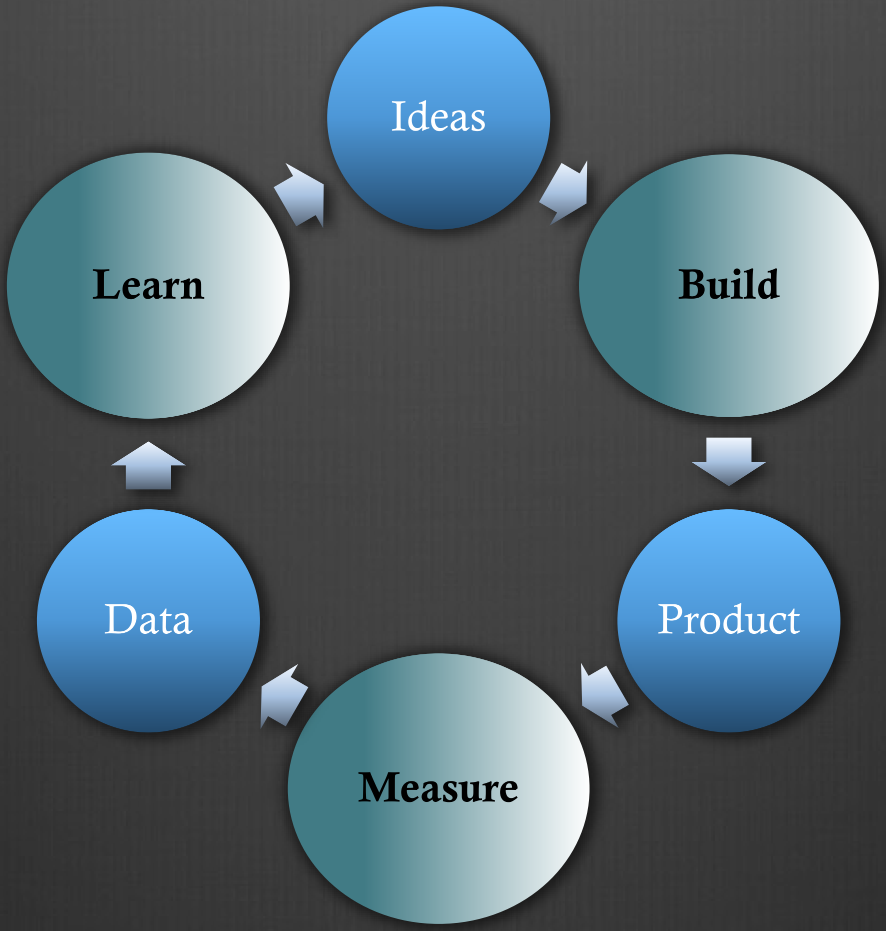
MVP…What's That?

- No, not the **Most Valuable Player**.
  - Although being one never hurts.
- For this strategy, it's the
  - Minimum
  - Viable
  - Product

Your “Strategy Starter”

- To kick off this whole creative process, go back to your organization and look at your **entire security program** as the MVP.
- “But we’ve got a lot of complexity, Dave!”
  - Yep, I hear ya.
- Chances are, you can still improve. A lot.
- Accept this, and look at your existing program as the beginning baseline (aka MVP).

Now…the Feedback Loop.



Ideas

Build

Product

Measure

Data

Learn

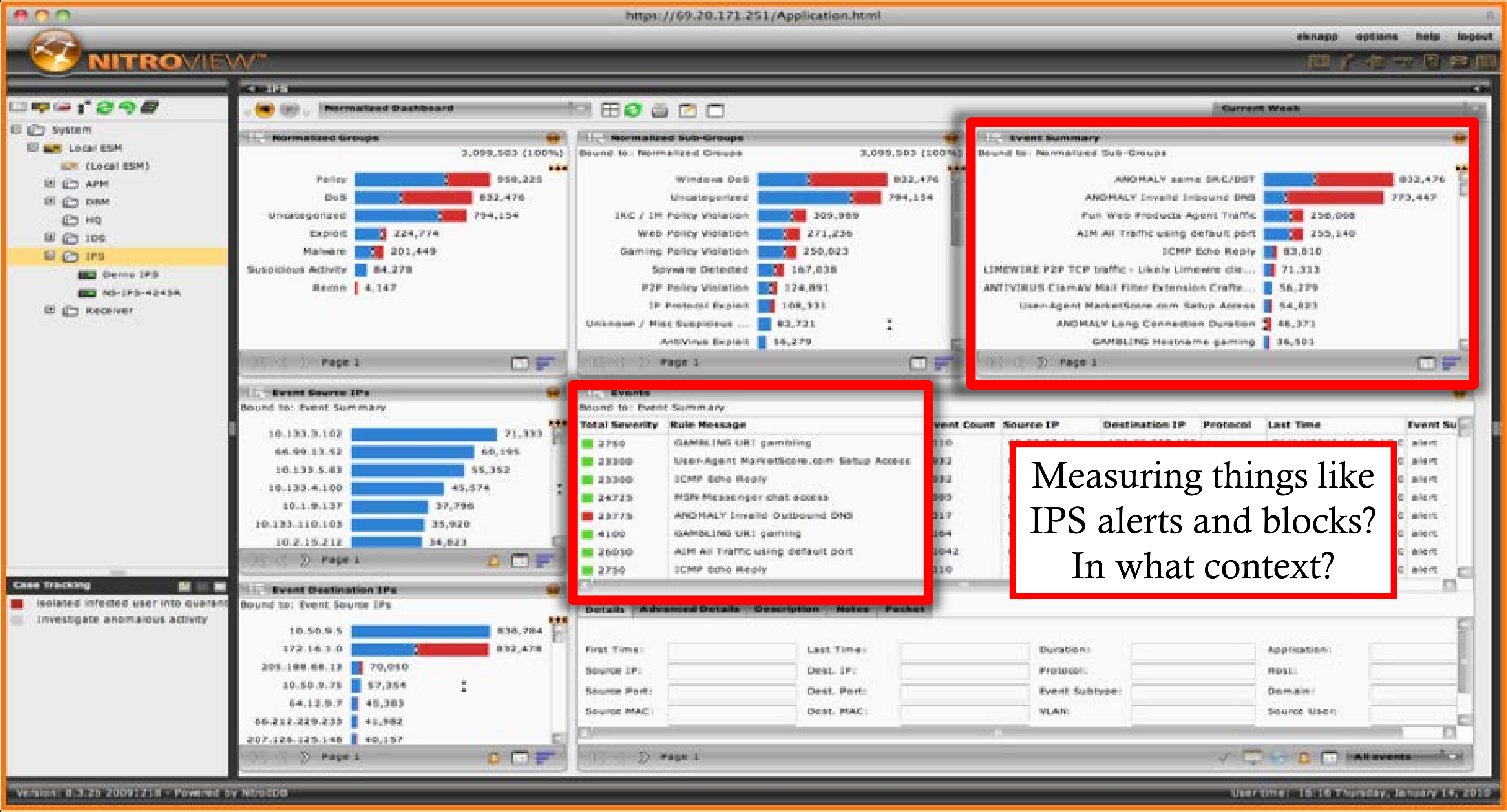
Building

- Build a program that helps to accomplish your goals, meeting your vision.
- **People**: Security should be unobtrusive wherever possible. People should also be protected.
- **Process**: Security should be as efficient as possible, and not interfere with business processes that drive revenue.
- **Technology**: All technology should be immediately tied to the security vision, with the goals of providing your "product" to the organization.

Measuring

- You need to measure how well you’re doing.
- All metrics should be:
  - **Actionable**: Every metric should be directly tied to causes and effects. No guessing. And actions should be possible based on them.
  - **Accessible**: Can all relevant stakeholder both easily SEE and UNDERSTAND your metrics? If not, revise them and make them available.
  - **Auditable**: Are your metrics credible? No “leaps of faith”.

Metrics Example



Case Tracking

- 🟥 Isolated infected user into quarant
- investigate anomalous activity

Events

Bound to: Event Summary

Total Severity	Rule Message
🟩 2750	GAMBLING URI gambling
🟩 23300	User-Agent MarketScore.com Setup Access
🟩 23300	ICMP Echo Reply
🟩 24725	MSN Messenger chat access
🟥 23775	ANOMALY Invalid Outbound DNS
🟩 4100	GAMBLING URI gaming
🟩 26050	AIM All Traffic using default port
🟩 2750	ICMP Echo Reply

First Time:
Last Time:
Duration:
Application:
Source IP:
Dest. IP:
Protocol:
Host:
Source Port:
Dest. Port:
Event Subtype:
Domain:
Source MAC:
Dest. MAC:
VLAN:
Source User:

Version: 8.3.20 20091218 - Powered by NitroEDB

User time: 16:16 Thursday, January 14, 2010

Measuring things like IPS alerts and blocks? In what context?

Learning

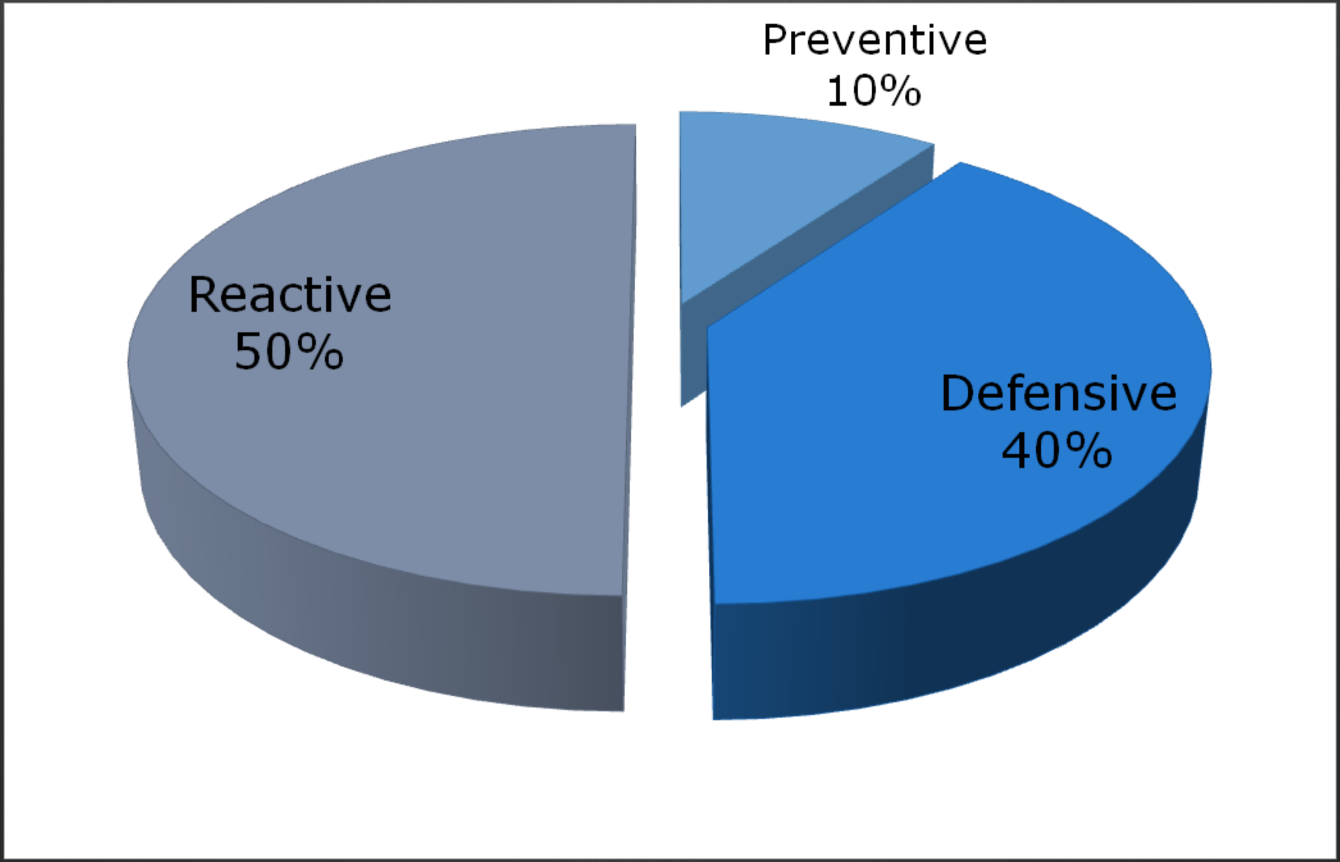
- Learning is the most valuable aspect of this cycle for infosec teams.
- A common entrepreneur excuse for failure: "Well, we learned a lot".
    - Maybe, but what did it lead to?
- Understand VALUE vs. WASTE.
- Also know MACRO learning (industry) vs. MICRO learning (your own organization)

A Final Point: Get Out More.

- No, really.
- We need lots of input for learning in infosec.
- Internal:
  - Users
  - IT
  - Business units
- External:
  - Partners
  - Threat info sources (SANS ISC, commercial services)
  - YOUR PEERS

Be More Proactive.

How most security shops spend their time.



Data Correlation & Analysis

- First things first: We have lots of data
- Detective and reactive solutions need to sift through this normalized data and find patterns that trigger events
- We're not doing a good job of telling "stories" or matching "real world" scenarios though.

Data Types

- System Access Logs
- Database/App Logs
- Network Device Logs
- IDS/IPS Events
- Vulnerability Assessments
- Behavioral Data (Flow, etc.)

```
Jan 20 11:54:15 [192.149.115.1]
%PIX-2-106001: Inbound TCP
connection denied from
1.2.3.47/47321 to a.b.c.d/111 flags
SYN on interface outside

Jan 20 11:55:25 [192.149.115.1]
%PIX-2-106001: Inbound TCP
connection denied from
1.2.3.47/4842 to a.b.c.d/135 flags
SYN on interface outside

Jan 20 11:54:15 [192.149.115.1]
%PIX-2-106001: Inbound TCP
connection denied from
1.2.3.47/38485 to a.b.c.d/445
flags SYN on interface outside
```

```
Jan 27 17:23:16 10.10.10.123 security[fai
Logon Failure: Reason:Unknown user na

Administrator  Domain:webserver1 Logon Type:3 Logon Process:User32
Authentication Package:Negotiate Workstation Name:
```

```
Oct 2 01:13:19 host sshd[19618]: Illegal user
test from ::ffff:69.10.144.194
Oct 2 01:13:19 host sshd[19618]: Address
69.10.144.194 maps to unknown.xyz.com, but
this does not map back to the address
POSSIBLE BREAKIN ATTEMPT!
```

```
080129 03:00:32 1 Connect websa@webserver1 on dbserver1
080129 03:01:48 1 Query show tables
080129 03:02:22 1 use creditcarddb;
080129 03:04:56 1 SELECT * FROM cardnumbers;
```

Changing our Risk Profile

- Today's attacks require a different focus:
  1. Prevention techniques should protect you from 80% or more of the issues
  2. Detection techniques should be focused on continuous monitoring
  3. Reaction capabilities are inevitable, and should be focused on speed and thoroughness
- With 90% Detection and Reaction - we are just doing "knee jerk" security
  - This is **bad**.

Prevention: Education

- Educating users about the dangers of the Internet (!) is important
    - Browsing safely
    - Not giving out personal or sensitive information over the phone
    - Separating work and personal life on social media networks
    - Being wary of links and emails with attachments
- However, many security awareness programs don’t seem to work well - why?

Prevention: Communication

- Risk needs to be articulated in audience-specific formats
- What are the best ways to communicate and work with groups internally & externally?
- **Internally**:
  - Proactive communications: Share news stories and new threat information with executive management, IT management, and employees (via newsletter or Intranet)
- **Externally**:
  - Develop and nurture contacts and relationships with law enforcement, ISP, and key partners and customers
  - Set a "threshold" or "trigger" for when to communicate potential issues

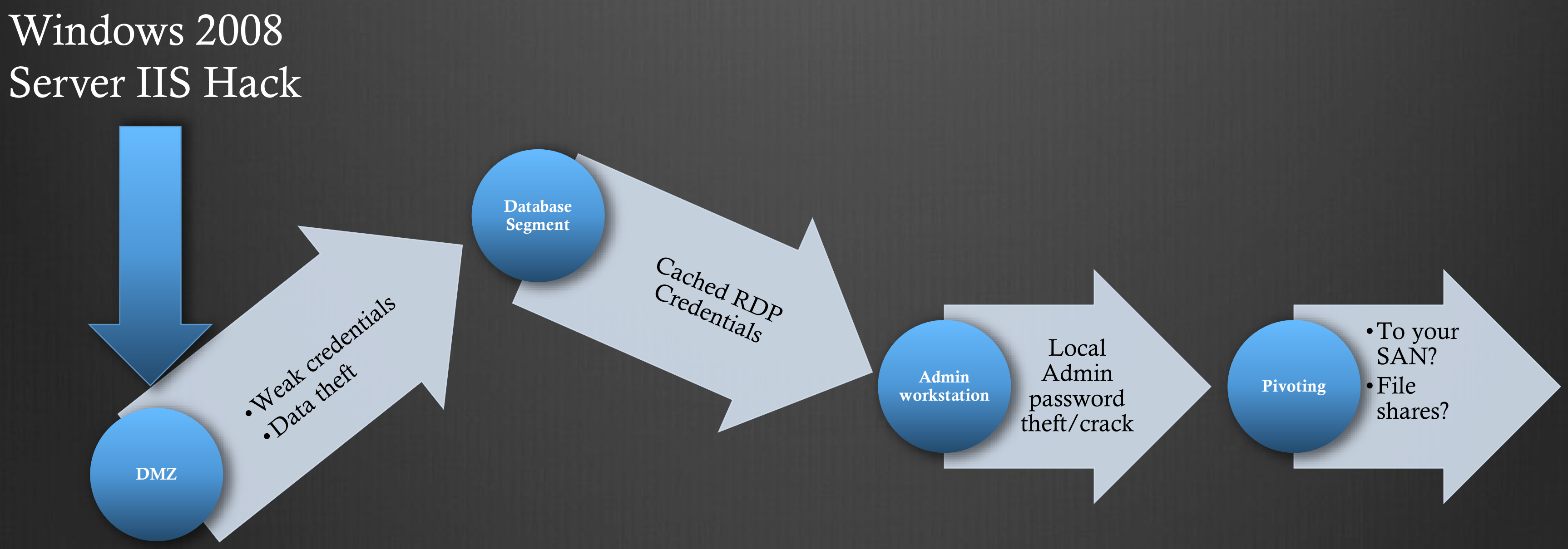
Prevention: Testing Yourself

- Find holes before attackers do!
- Prove that security issues exist to skeptical management
- Raise overall **security awareness**
- Verify secure system configurations
- Test new technology
- Discover gaps in compliance posture and satisfy legal, industry and/or governmental requirements such as HIPAA, SOX or PCI DSS.

It’s never this simple.

- OK, so these are the basics.
- We have two much bigger issues, that tie back to the way we think.
  - We WAIT for input to learn from.
  - We do not model REAL-WORLD scenarios that depict how our PRODUCT will serve our CUSTOMERS.
- **We will never, ever get there by just gathering data from sensors and dashboards.**

Real Threat Modeling?



What about social engineering with your users? Behavioral monitoring?

Suggestions

- For Building:
  - Only buy technologies that help your “product”
  - Be prepared to “pivot” in your strategy - no “status quo”
- For Measuring:
  - Define metrics that are actionable, accessible, and auditable
  - Put all metrics in context - more data is not necessarily better
- For Learning:
  - Model threats and perform real-world attack scenarios
  - Get out more to get input and feedback - users and peers

A Final Thought

- Gene Kim, a friend and all around “smart guy”, just said this in his SXSW presentation last weekend:

  “There is a disastrous consequence of status quo.”

- Folks, this is true.
- Leadership != Meetings + Politics
- Creative Security (startup mentality) != Ramen Noodles and a Garage

Final Discussion & Questions

Thanks for attending!