

# Budgeting for Common-Sense Computer Security in Financially Tight Times

Javed Ikbal & Craig Brown  
zSquad

Identify :: Align :: Remedy :: Verify :: Secure



# About zSquad

- Information Security Consulting Practice
- Focus areas are:
  - Policy review/development
  - IT Governance
  - Penetration testing / audit
  - Security Architecture
  - Application Security
  - PCI, SAS 70 and ISO 27001 audit prep
  - 3rd party due diligence audits
  - Training (Secure coding, Awareness)
- Customers are mostly financial services, insurances and state / city agencies

# Agenda

- We don't need no stinkin' information security
  - We have nothing hackers want
  - Or do we?
- So how do we...?
- So what do we... And how much?
  - Policy!
  - User Education
  - Testing
  - Acceptable Use Policy
  - Documented distribution
  - Patching
  - Managing User Accounts
  - Security Recommendation for Home

**We don't need no stinkin'  
information security...**

**we have**

**Nothing**

**hackers want**

**Right?  
Wrong!**

# Government Information

- Government information is mostly public
  - Subject to “Right to know” (certain exceptions)
  - Most information, such as salary, is public
  - No trade secrets or business confidential information
- 
- Do we need information security?

# Confidential? Not Confidential?

- Taxes
- Penalties
- Liens
- Education records
- Library borrowing records
- Credit card numbers used to pay bills
- Bank account number (from checks)
- Employee social security numbers
- Citizen social security numbers
- Social services records
- Prisoner movement
- Etc, etc.

# How Serious is the Threat?

- 1,500,000,000 Internet users
- 1000 new viruses per month
- 2 billion “phishing” emails per month
- 1 million PCs with trojan malware installed, ready to be remote-controlled by the bad guys
- More than 100 million identities breached in 2007
- 2008 and 2009—more than 150 million identity breaches

# ID Theft In New Hampshire

From the Nashua Telegraph, February 22, 2008

## Woman jailed in identity theft

“A Hudson woman posed as another woman as she illegally obtained a prescription drug and merchandise with a stolen credit card, city police said.”

# It Happens At City Halls

Consultant's stolen laptop had personal information, including social security numbers for as many as 280,000 retired New York City employees.

Twenty-six IRS tapes missing from Kansas City's City Hall

# It Happens At City Halls-2

- Town of Sandwich, Massachusetts lost \$50,000 in November 2008
- A software that captured every single keystroke (a “keylogger”) got installed on the town treasurer’s computer
- It captured and sent the web-banking userid and password to the hackers
- Who used that to transfer \$50,000 to various banks in Florida and Georgia
- An unwitting accomplice (a “mule”) who thought he was getting an accounting job opened the accounts, and transferred the funds to St. Petersburg, Russia.

| Company                            | Date   | Year |
|------------------------------------|--------|------|
| <u>Williams College</u>            | 30-Oct | 2009 |
| <u>Easybakeware</u>                | 19-Oct | 2009 |
| <u>Radisson</u>                    | 12-Oct | 2009 |
| <u>Vernon Sales Promotion</u>      | 12-Oct | 2009 |
| <u>Verso Paper Corp</u>            | 28-Sep | 2009 |
| <u>AlixPartners</u>                | 16-Sep | 2009 |
| <u>T. Rowe Price Services Inc.</u> | 15-Sep | 2009 |
| <u>Express Scripts, Inc.</u>       | 14-Sep | 2009 |
| <u>MassMutual Financial Group</u>  | 8-Sep  | 2009 |
| <u>KSM Business Services Inc</u>   | 4-Sep  | 2009 |
| <u>Hilton</u>                      | 3-Sep  | 2009 |
| <u>T-Mobile</u>                    | 3-Sep  | 2009 |

Source: <http://doj.nh.gov/consumer/breaches.html>



| Company                                   | Date   | Year |
|---|--------|------|
| <a href="#">Williams College</a>          | 30-Oct | 2009 |
| <a href="#">Easybakeware</a>              | 19-Oct | 2009 |
| <a href="#">Radisson</a>                  | 12-Oct | 2009 |
| <a href="#">Vernon Sales Prom</a>         | 2-Oct  | 2009 |
| <a href="#">Verso Paper Corp</a>          | 8-Sep  | 2009 |
| <a href="#">AlixPartners</a>              | 6-Sep  | 2009 |
| <a href="#">T. Rowe Price Serv</a>        | 5-Sep  | 2009 |
| <a href="#">Express Scripts, In</a>       | 1-Sep  | 2009 |
| <a href="#">MassMutual Finan</a>          | 1-Sep  | 2009 |
| <a href="#">KSM Business Services Inc</a> | 4-Sep  | 2009 |
| <a href="#">Hilton</a>                    | 3-Sep  | 2009 |
| <a href="#">T-Mobile</a>                  | 3-Sep  | 2009 |

**74 in 2009**  
**119 in 2008**  
**114 in 2007**

| Company                                     | Date   | Year |
|---|--------|------|
| <a href="#">Williams College</a>            | 30-Oct | 2009 |
| <a href="#">Easybakeware</a>                | 19-Oct | 2009 |
| <a href="#">Radisson</a>                    | 12-Oct | 2009 |
| <a href="#">Vernon Sales Prom</a>           |        | 2009 |
| <a href="#">Verso Paper Corp</a>            |        | 2009 |
| <a href="#">AlixPartners</a>                |        | 2009 |
| <a href="#">T. Rowe Price Services Inc.</a> |        | 2009 |
| <a href="#">Express Scripts, Inc.</a>       |        | 2009 |
| <a href="#">MassMutual Financial</a>        |        | 2009 |
| <a href="#">KSM Business Services Inc</a>   |        | 2009 |
| <a href="#">Hilton</a>                      | 3-Sep  | 2009 |
| <a href="#">T-Mobile</a>                    | 3-Sep  | 2009 |

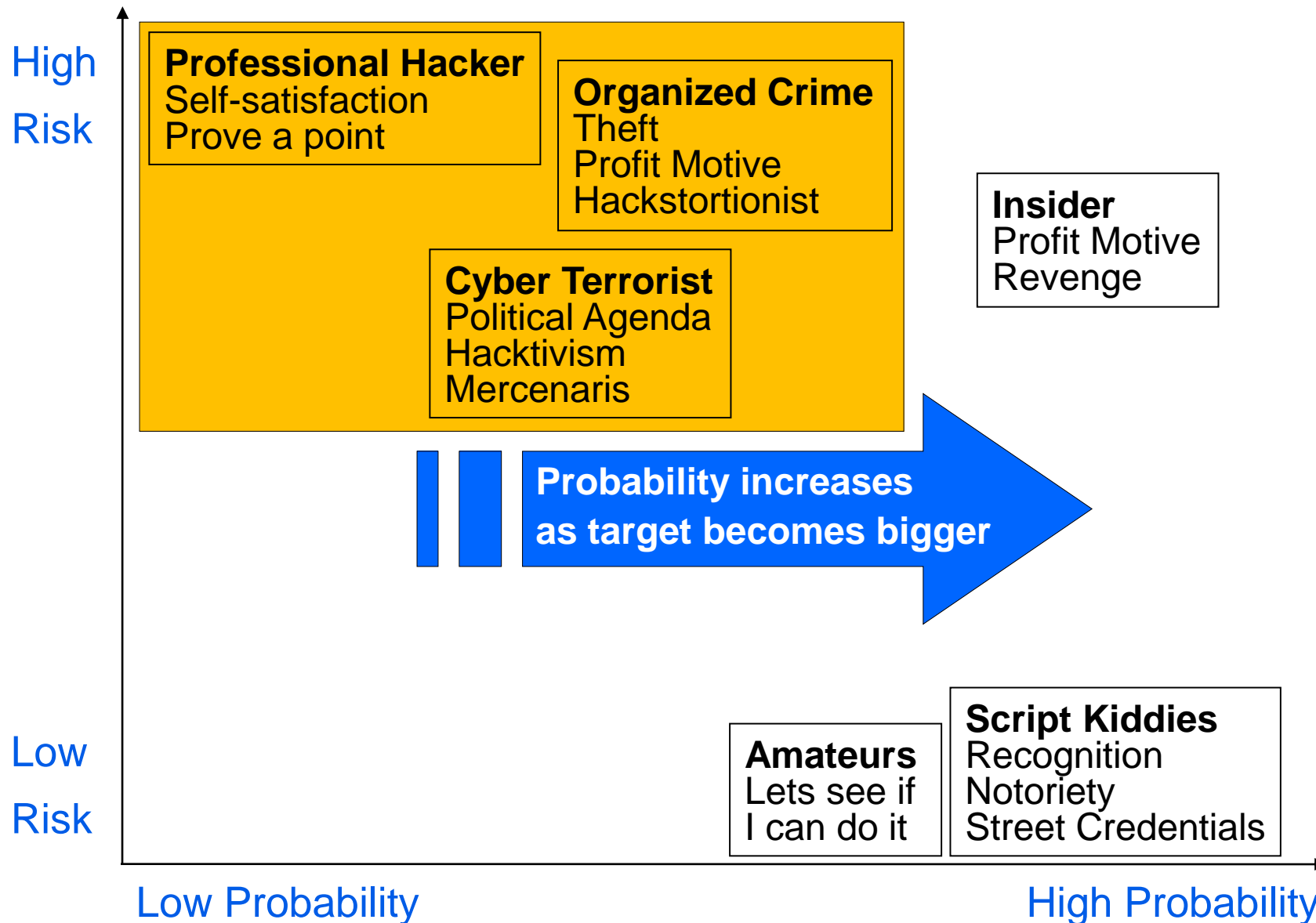
**And we hope  
you did not stay  
at these chains**

# You have similar information

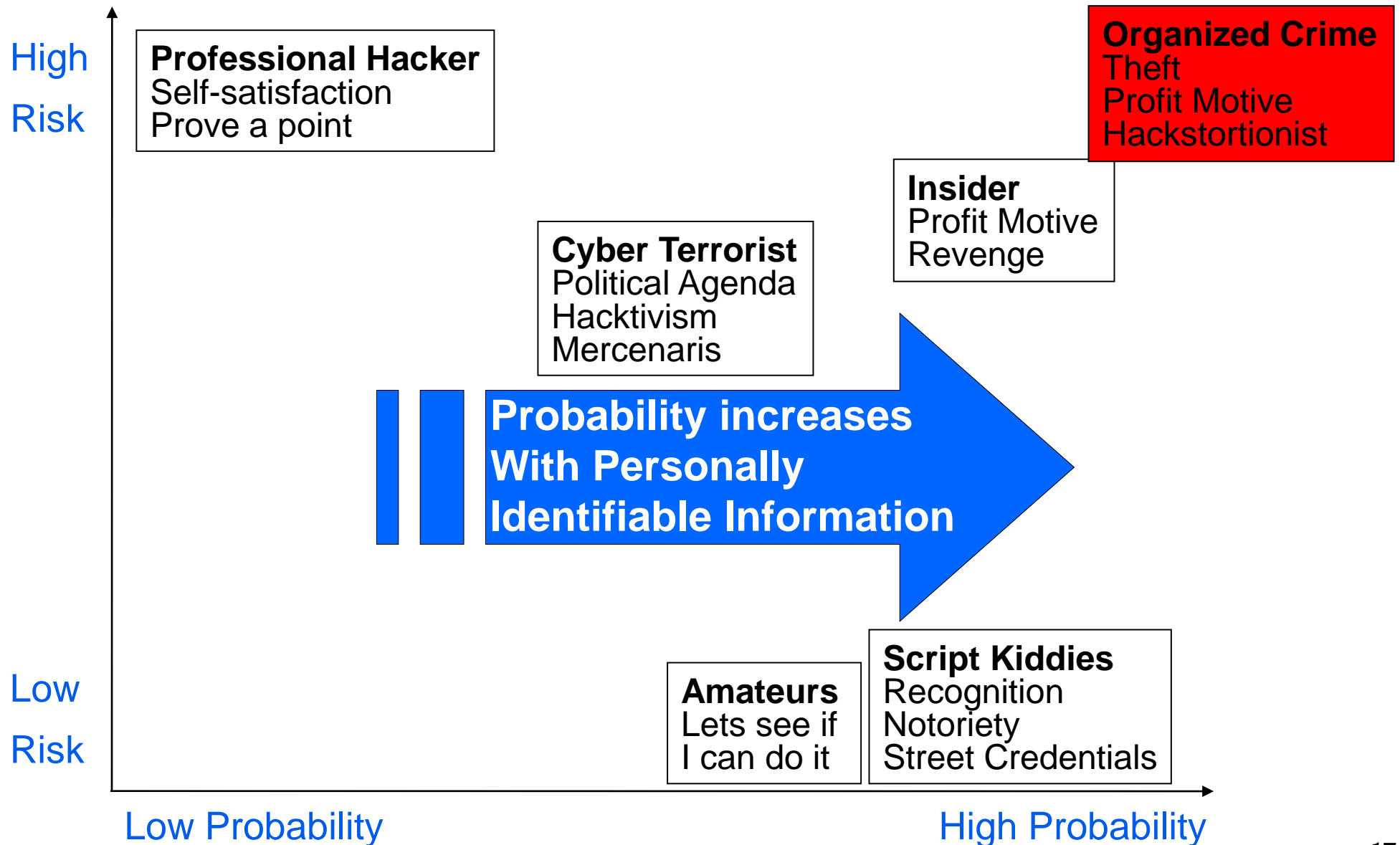
- **Name**
- **Address**
- **Social Security Numbers**
- **Credit Card Numbers**
- **Bank Account numbers**

**And the bad guys  
know it**

# Why People Hacked – 2004 Edition



# Why People Hack – 2009 Edition



**Lets meet**

**“Bud”**

**[Click to view](#)**

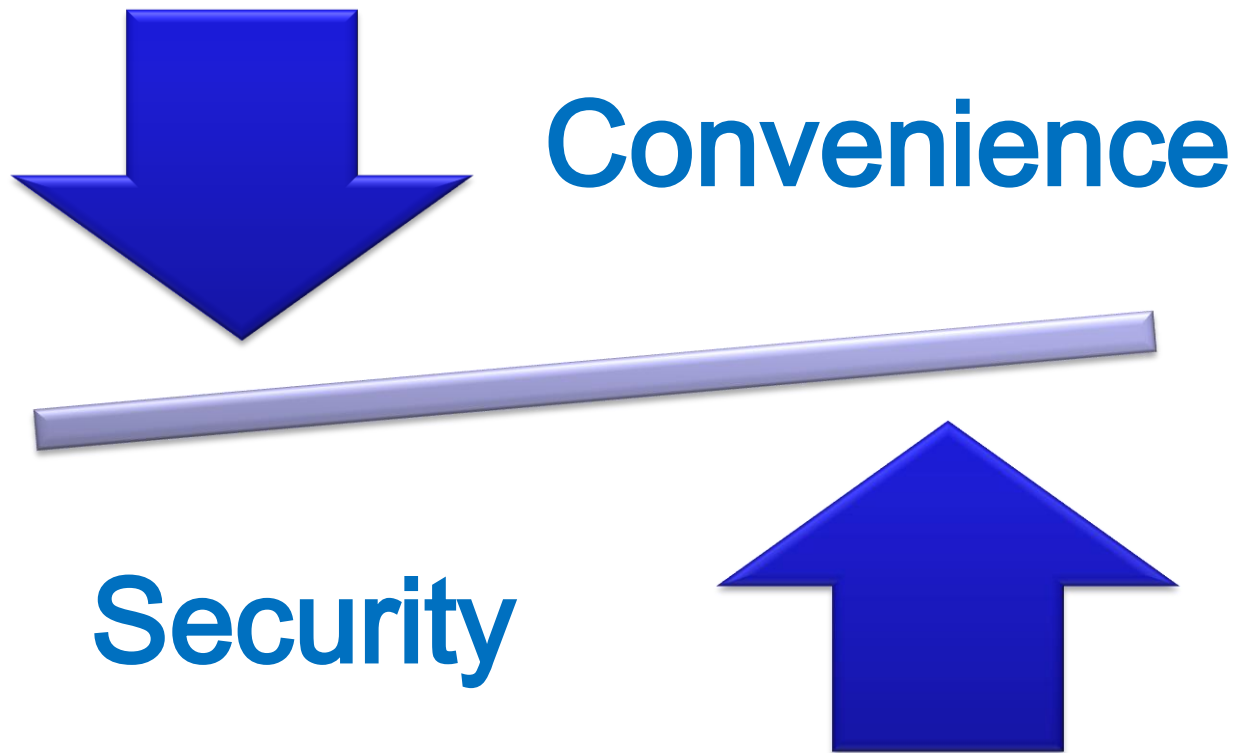
**Do you have a  
“Bud”?**

**Then you have an  
Opportunity  
for  
Improvement**

# Drivers for Information Security



# Does Security Get in the Way?



Do you hate it when your screen locks after inactivity?

# We Are Here Because

- Technology is easy
- People are not
- We are the final defense
- We share the responsibility



**We are the final firewall**

# Do You Know?

- Where you have confidential information?
  - Which employees have access to it?
  - Have they been trained to not give out information to unauthorized people?
- Is there an acceptable use policy at work?
  - Do you have signatures to prove that the employees have received a copy?
- Virus, worms, phishing
  - Have the employees been trained?

**Do you monitor  
confidential information access?**

**Would you know  
If  
your data gets stolen?**

- **Simple**
- **Good**
- **Inexpensive**

**Yes, you can have all 3**

Disclaimer: may not need hard \$,  
but you will need to spend time on these.

# 1. Start With A Policy

- (if you don't have one, that is)
- It should:
  - Name the position responsible for security
    - (does not have to be dedicated to security)
  - Show management support for security
  - Spell out that your organization is committed to protecting confidential information
  - Define information security roles and responsibilities
  - Be reviewed once a year
- Free templates available:
  - <http://www.sans.org/security-resources/policies/>
  - Or ask your peers

Policy: \$0

-----  
Total: \$0

## 2. Train Your Users

Social Engineering over the Phone: Cracking an Account

Click to [watch on YouTube](#)

Policy: \$0  
Training: \$0

---

**Total: \$0**

## 2. Train Your Users

- Bad things could happen without training
- At a client, we tried the exact same approach
- The results were so bad, it was called off after the first few phone calls
- 3 most important lessons you can share:
  - Do not share your password
  - Lock your computer
  - Do not data on portable drives and laptops (and phones)

Policy: \$0

Training: \$0

-----  
**Total: \$0**

## 2. Train Your Users

Do your users know not to leave laptops unguarded?

Click to [watch on YouTube](#)

Policy: \$0

Training: \$0

---

**Total: \$0**

## 2. Training: Good, Free Resources

- Youtube (If allowed from work)
- Search for “social engineering” or “information security”—embed them on your Intranet
- Newsletter: Lots of free articles
- Commonwealth of Virginia: The Duhs of Security

Policy: \$0

Training: \$0

---

**Total: \$0**

## 2. Training: The Duhs of Security

<http://www.vita.virginia.gov/security/>

Click to [watch on YouTube](#)

Policy: \$0  
Training: \$0

---

**Total: \$0**

# 3. Acceptable User Policy (AUP)

- People are shocked to find out that they have no right to privacy in their communications when using employer's equipment
- Yes, even in New Hampshire
- Free templates available, also from your peers
- Final version to be developed jointly between HR, Legal and IT
- Employees do not have to agree to the policy, they just have to sign a document stating they have received, read and understood the policy
- Dig this well before you are thirsty

Policy: \$0

Training: \$0

AUP: \$0

---

**Total: \$0**

# 3. Audit Windows Infrastructure

- MBSA: Microsoft Baseline Security Analyzer
  - <http://technet.microsoft.com/en-us/security/cc184923.aspx>
- Find weak passwords, missing security patches
- Regularly patch Windows servers
- Configure servers securely.
- Secure configuration checklist:
  - <http://cisecurity.org/>

Policy: \$0  
Training: \$0  
AUP: \$0  
Windows Audit: \$0  
-----  
**Total: \$0**

## 4. Manage Add/Change/Delete

- Do you have live accounts for users who left 6 months ago?
- Why?
- Establish electronic or paper forms for each user add/change/delete request
- Document each request

Policy: \$0

Training: \$0

AUP: \$0

Windows Audit: \$0

User Mgmt: \$0

---

**Total: \$0**

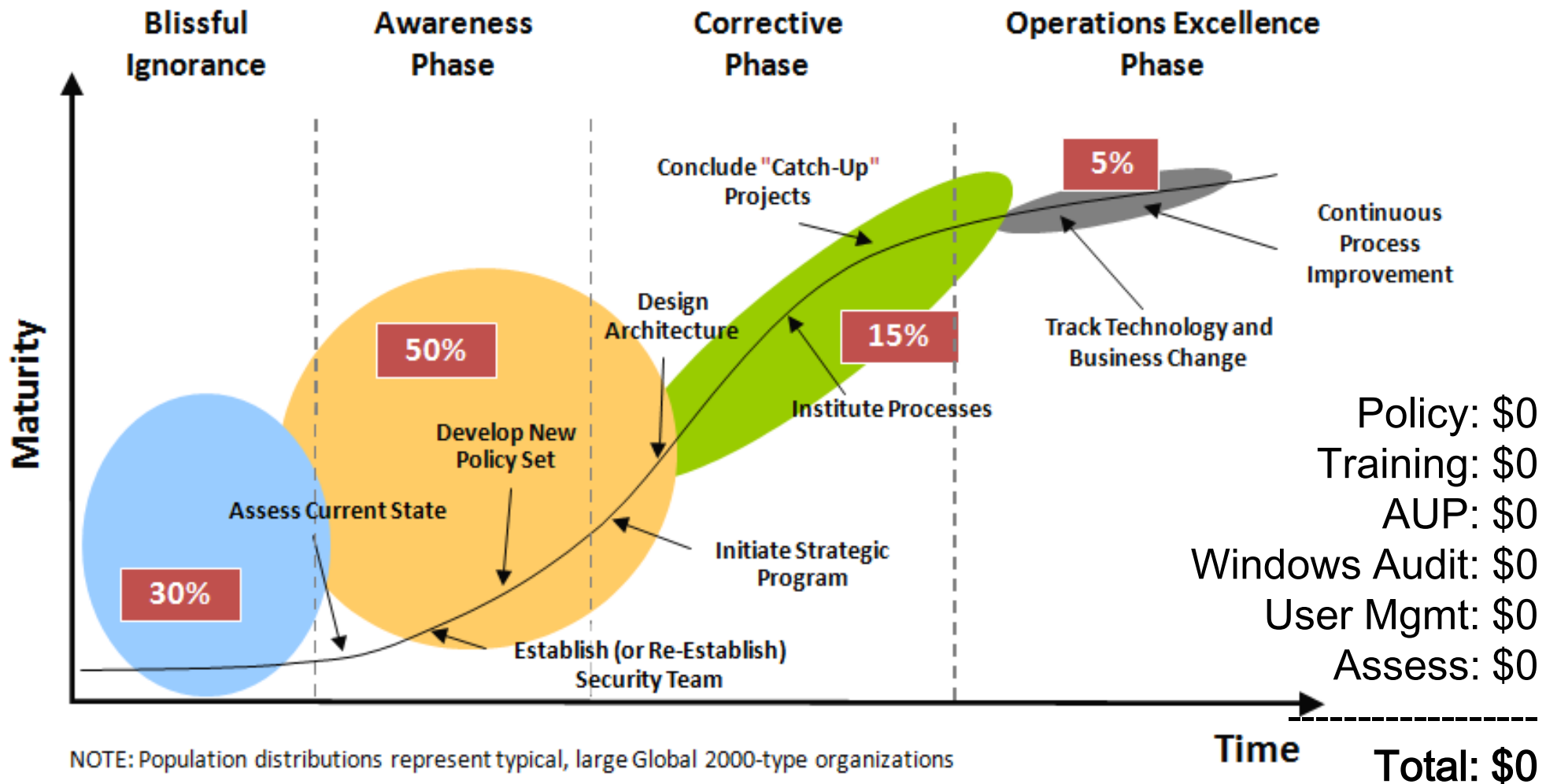
35

# 5. Install Anti-Virus

- Like patches, AV needs to be updated
- An AV product without the latest patches is worse than no AV product at all.
- Because it gives a false sense of security
- Lots of good, free AV products for home use
- Encourage users to use them on their personal computers if they are already not using one

Policy: \$0  
Training: \$0  
AUP: \$0  
Windows Audit: \$0  
User Mgmt: \$0  
Home AV: \$0  
-----  
**Total: \$0**

# Stop And Assess



# 6. Assess Network, Website

- If you have completed the preceding items
- Do it if you are approaching the corrective phase
- Needed to know where you are, and where you should go next
- May need external resources
- Will require planning and project management
- Do NOT do it until you are ready to address the findings
- Knowledge + Inaction = Liability
- This also means having the funds to fix
- This is optional.

|                  |              |
|------------------|--------------|
| Policy:          | \$0          |
| Training:        | \$0          |
| AUP:             | \$0          |
| Windows Audit:   | \$0          |
| User Mgmt:       | \$0          |
| Assess Progress: | \$0          |
| Ext. Assessment: | \$10K        |
| -----            |              |
| <b>Total:</b>    | <b>\$10K</b> |

# 7. Test Users

- Could be in-house social engineering test
  - Or external resources
  - Something as simple as a fake IRS email
  - Or elaborate phone tests
  - Do not forget to walk around and look under keyboards

|                  |              |
|------------------|--------------|
| Policy:          | \$0          |
| Training:        | \$0          |
| AUP:             | \$0          |
| Windows Audit:   | \$0          |
| User Mgmt:       | \$0          |
| Assess Progress: | \$0          |
| Ext. Assessment: | \$10K        |
| Test Users:      | \$0          |
| -----            |              |
| <b>Total:</b>    | <b>\$10K</b> |

## 8. Establish Change Management

- Document each change in the production environment
- Also document the reason for change and the approval process.

|                    |              |
|--------------------|--------------|
| Policy:            | \$0          |
| Training:          | \$0          |
| AUP:               | \$0          |
| Windows Audit:     | \$0          |
| User Mgmt:         | \$0          |
| Assess Progress:   | \$0          |
| Ext. Assessment:   | \$10K        |
| Test Users:        | \$0          |
| Change Management: | \$0          |
| -----              |              |
| <b>Total:</b>      | <b>\$10K</b> |

# 9. Train IT Staff

- If you do inhouse software development, train the developers
  - If you have a web-programmer, s/he also needs to be trained
  - It is very easy to write web applications that can be broken into
- Train system and network administrators in basic security practices for the platforms they manage

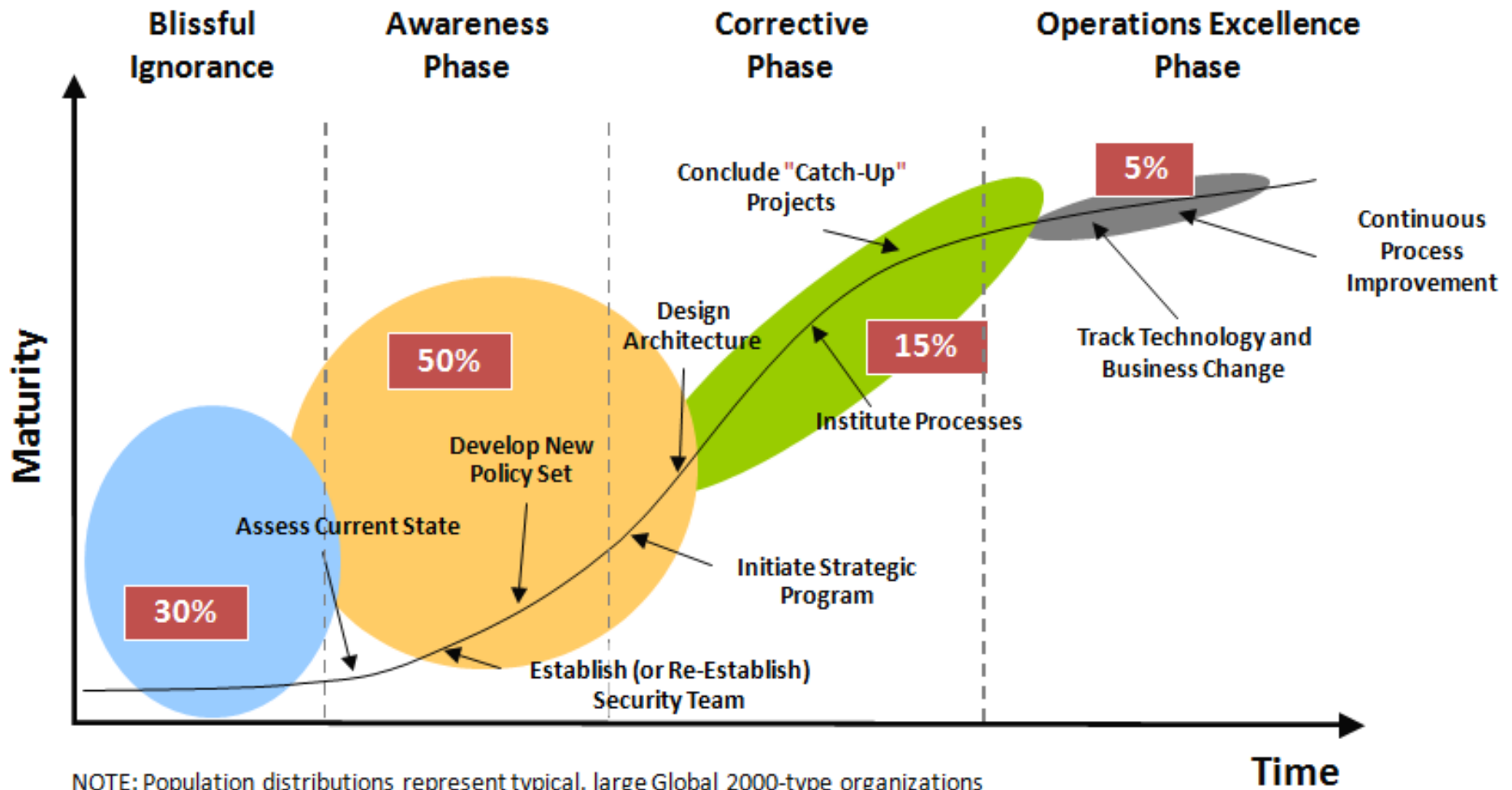
|                    |              |
|--------------------|--------------|
| Policy:            | \$0          |
| Training:          | \$0          |
| AUP:               | \$0          |
| Windows Audit:     | \$0          |
| User Mgmt:         | \$0          |
| Assess Progress:   | \$0          |
| Ext. Assessment:   | \$10K        |
| Test Users:        | \$0          |
| Change Management: | \$0          |
| Train IT Staff:    | \$0          |
| -----              |              |
| <b>Total:</b>      | <b>\$10K</b> |

# 10. Assess Vendors

- If you send confidential information to vendors, ask them about their information security practices.
- Your best security is useless if the information gets stolen from the vendor
- Questionnaire available:
  - <http://www.sharedassessments.org/download/>

|                    |              |
|--------------------|--------------|
| Policy:            | \$0          |
| Training:          | \$0          |
| AUP:               | \$0          |
| Windows Audit:     | \$0          |
| User Mgmt:         | \$0          |
| Assess Progress:   | \$0          |
| Ext. Assessment:   | \$10K        |
| Test Users:        | \$0          |
| Change Management: | \$0          |
| Train IT Staff:    | \$0          |
| Assess Vendors:    | \$0          |
| -----              |              |
| <b>Total:</b>      | <b>\$10K</b> |

# Congratulations: Green Zone



Policy: \$0  
Training: \$0  
AUP: \$0  
Windows Audit: \$0  
User Mgmt: \$0  
Assess Progress: \$0  
(Optional, but recommended)  
Ext. Assessment: \$10K  
Test Users: \$0  
Change Management: \$0  
Train IT Staff: \$0  
Assess Vendors: \$0  
-----  
Total: \$10K

# Questions?

**[www.zsquad.com/download](http://www.zsquad.com/download)**

**[javed@zsquad.com](mailto:javed@zsquad.com)**

**[craig@zsquad.com](mailto:craig@zsquad.com)**