



# Security in knowledge

## CASE STUDY: MANAGING TRUST & RISK

**Bryan Green**

Manager, Directory Engineering  
CME Group

**Mike Wolfe**

Senior Security Architect  
Blue Shield of California

Session ID: SPO2-W21

Session Classification: Intermediate

# MANAGING TRUST & RISK

Bryan Green, CME Group



# LEARNING OBJECTIVES

- ▶ Building the Business Case for Trust
- ▶ Building Trust
- ▶ Maintaining Trust
- ▶ Lessons learned and what you can do starting next week!

# ABOUT CME GROUP

- ▶ Worlds largest and most diverse futures exchange in the world.
- ▶ CME Group is comprised of
  - ▶ Chicago Mercantile Exchange (CME)
  - ▶ Chicago Board of Trade (CBOT)
  - ▶ New York Mercantile Exchange (NYMEX)
  - ▶ Commodities Exchange (COMEX)
- ▶ Where the world comes to manage risk

# ABOUT CME GROUP

- ▶ Highly Regulated Industry
  - ▶ Commodities Futures Trading Commission (CFTC)
  - ▶ Securities and Exchange Commission (SEC)
- ▶ The Numbers
  - ▶ 13.4 Million Average Daily Trades
  - ▶ 3.4 Billion Contracts Traded in 2011
  - ▶ Over \$1 Quadrillion in Notational Value in 2011
    - ▶ 1 Quadrillion = 1000 Trillion

# BUILDING THE BUSINESS CASE

- ▶ **Move to common authentication scheme**
  - ▶ Replace PAC files
  - ▶ Replace RSA Tokens
  - ▶ Lower authentication TCO
- ▶ **Replace RSA Token after 2011 breach in trust**
  - ▶ Bring security controls in house
- ▶ **Improve existing PKI assurance**

# BUILDING TRUST

- ▶ **Build PKI with a high level of assurance**
  - ▶ Secured with offline CAs
  - ▶ Secured with Hardware Security Modules
  - ▶ Secured with multi-party authentication



# BUILDING TRUST

- ▶ Documented Processes
- ▶ Audited
- ▶ Enterprise Key and Certificate Management





# MAINTAINING TRUST

*“Trust can take years to build, seconds to destroy, and forever to repair.”*


*- Unknown*



# MAINTAINING TRUST

- ▶ What can break trust?
  - ▶ **Lax Access Controls**
    - ▶ Who has access to your private keys? Are you sure? Can you prove it?
  - ▶ **Antiquated Security Standards**
    - ▶ Insecure hashing algorithms
    - ▶ Outdated Key Length




# DEMO: POLICY ENFORCEMENT

**CSR Validation**  Symantec. How to generate a CSR

Paste your CSR into the box and click 'Validate'. Your CSR should start with  
-----BEGIN CERTIFICATE REQUEST-----  
and end with  
-----END CERTIFICATE REQUEST-----

Your CSR Details will be shown below.

**Validate**

 **CSR Validator**     **Certificate Checker**     **sslToolbox**

Copyright © 2011 Symantec Corporation. All rights reserved. | [Legal Notices](#) |

# DEMO: POLICY ENFORCEMENT

▶ <https://ssl-tools.verisign.com/#csrValidator>

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIBYjCCATMCAQAwYkxCzAJBgNVBAYTAiVTMQswCQYDVQQIEwJJTDEQMA4GA1UEBxMHQ2hpY2Fn
bzESMBAGA1UEChMJQ01FIEdyb3VwMQ0wCwYDVQQLEwRFVFBBMSEwHwYJKoZIhvcNAQkBFhJub29u
ZUBjbWVncm91cC5jb20xFTATBgNVBAMMDCouZ29vZ2xlLmNvbTCBnzANBgkqhkiG9w0BAQEFAAOB
jQAwYkCgYEAqAC6Fu1s3K+zwouWkxcnWISseZ49bE9bMc916GU7rbX7dUR4OUCLMtTX6FGxeam8
Nnt9zd8F3RZjKN2LY7q8IMTKWZ42snuHhJ3Xr6CJ5Y8rX7/vuwCt2Os4DGM261Io6Bi9ns9eVDJE
Rq6h055TI0sDTVrLvIWQScTXkl6TNo0CAwEAaAAMA0GCSqGSIb3DQEBAUAA4GBACSDXSv4fRIL
6l1v0qz3DQ89VHVtcMXkgRnNN2zL/EY6FJgumv2VKIBcvdB+ECNowWgdBOzBFjZOlvyux2jEBbO9
/vkojVwrG+xl4G1Zeh5vMLvbc3sD+NK50+aKYZ/Sq8sEyMFWxbzEk8Zi5nV/TO+jWFe+3cDpLKdh
Yt1H4aQ+
-----END NEW CERTIFICATE REQUEST-----
```

# POLICY ENFORCEMENT: EVEN BETTER

The screenshot displays the Venafi Encryption Director web interface in Internet Explorer. The browser address bar shows `http://localhost/VEDAdmin/MyDashboard.aspx`. The interface includes a navigation menu with 'My Dashboard', 'Discover', 'Manage', and 'Help'. The main content area is titled 'Enterprise Apache : Settings' and features several tabs: 'Certificate', 'Monitoring', 'Validation', and 'General'. The 'Certificate' tab is active, showing a 'General Information' section with the following details:

- Description: (empty text box)
- Contact(s): AD+TAD:alice (CN=Alice, CN=Users, DC=training, DC=local) local:Admin (\VED\Identity\Admin)
- Approver(s): AD+TAD:bob (CN=bob, CN=Users, DC=training, DC=local) local:Admin (\VED\Identity\Admin)
- Processing Disabled:
- Management Type: Monitoring

Below the 'General Information' section is the 'CSR Handling' section, which includes:

- CSR Generation:  Service Generated CSR,  User Provided CSR
- Generate Key/CSR on Application: No
- Upload CSR button

The 'Subject DN' section at the bottom contains:

- Common Name: apache.training.local
- Subject Alt Name (DNS): (empty text box)
- Organization: Internet Widgits Pty Ltd
- Organization Unit: Training
- Save button

The left sidebar shows a tree view of policies, with 'Enterprise Apache' selected. The status bar at the bottom indicates 'Local intranet | Protected Mode: Off' and a zoom level of 100%.

# POLICY ENFORCEMENT: EVEN BETTER

	CERTIFICATE VALUE	RENEWAL VALUE	
Common Name:	apache.training.local	apache.training.local	
Subject Alt Name (DNS):			
Organization:	Internet Widgits Pty Ltd	Internet Widgits Pty Ltd	
Organization Unit:		Training	
City:		Sandy	
State:	Some-State	Utah	
Country:	AU	US	
Key Strength (bits):	1024	2048	

Other Information

Certificate Authority: apache.training.local

Public Key Algorithm: rsaEncryption

Signature Algorithm: sha1RSA

Set central policies to eliminate errors, mistakes, guesswork, audit violations, and much worse

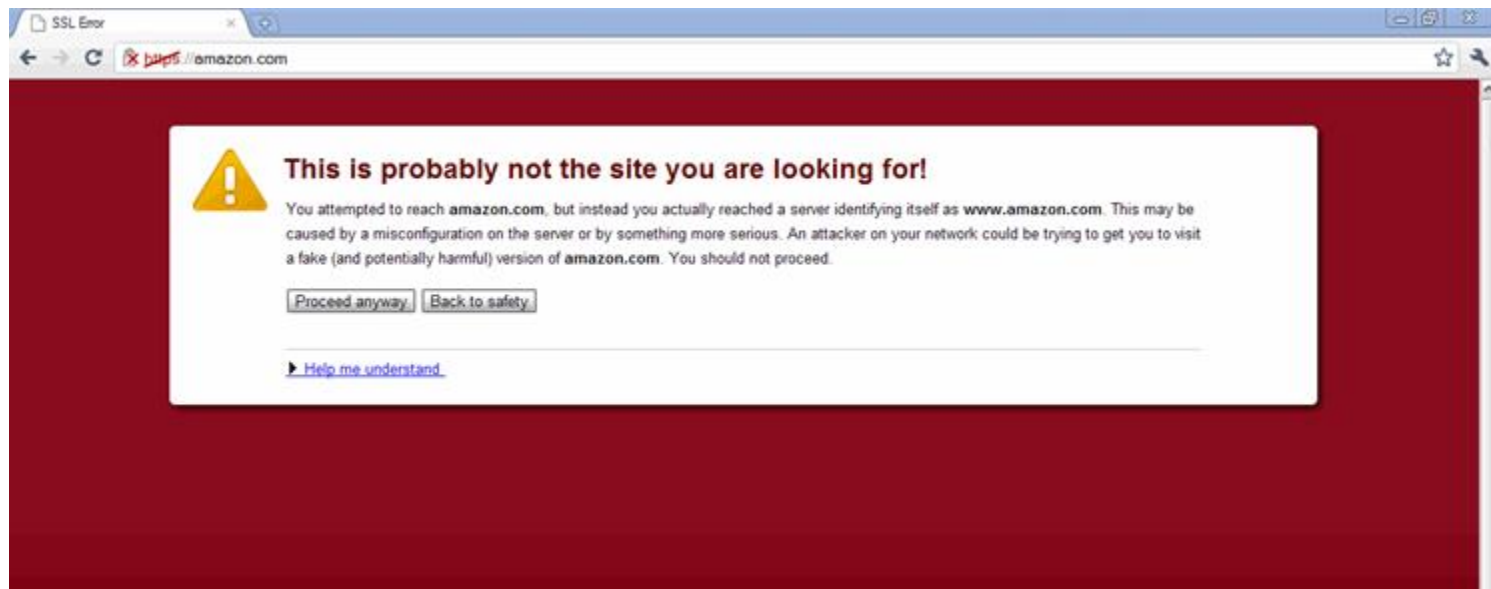
# MAINTAINING TRUST

- ▶ What can break trust?
  - ▶ **Poor Key and Certificate Management**
    - ▶ Expired Certificates
    - ▶ Certificate CN mismatches.



# MAINTAINING TRUST

- ▶ Don't let this be you!





# LESSONS LEARNED

## What We Didn't Know

- ▶ **Level of required processes**
  - ▶ Documentation
  - ▶ Key Transport
- ▶ **Cross Organizational Engagement Creates Trust**
- ▶ **Trust Creates Demand**



# LESSONS LEARNED

## How Our Process is Changing

### ▶ **Built-in**

- ▶ Policy enforcement
- ▶ Visibility & tracking

### ▶ **Support many, many different use cases**

- ▶ Devices
- ▶ Encryption v. authentication

### ▶ **When to use Internal v. Hosted PKI**

- ▶ Less reliance on hosted PKI



# LESSONS LEARNED

What's next for CME Group

▶ **Figuring out what we have**

- ▶ Venafi Director for Internal and External Inventory Scans

▶ **Prioritizing demand**

- ▶ With limited PKI SMEs we have to prioritize.

▶ **Internal Education**

- ▶ PKI is voodoo!

▶ **Automate, automate, automate!**

- ▶ Policy Enforcement
- ▶ Enrollment
- ▶ Self Service



# LESSONS LEARNED

## What's next for Your Organization?

### ▶ **Today**

- ▶ Do you have an internal PKI?
- ▶ What is the current state of your PKI?

### ▶ **3 Months**

- ▶ Plan for certificate based encryption and authentication
- ▶ Develop your business case!

### ▶ **6 Months**

- ▶ Budget money
- ▶ Budget time
- ▶ Engage SMEs for help. If you don't get it right the first time, there can't be any trust!

# **MANAGING TRUST & RISK**

**Mike Wolfe, Blue Shield of California**



# LEARNING OBJECTIVES

- ▶ Building the Business Case for Trust
- ▶ Building Trust
- ▶ Maintaining Trust
- ▶ Lessons learned and what you can do starting next week!

# — ABOUT Blue Shield of California

- ▶ Part of Blue Cross Blue Shield Association (BCBSA), serving our “Blue” members in California
- ▶ Medical Claims Processor: key player in new California Healthcare Exchange under Affordable Health Care Act.
- ▶ Shifting from out-sourced EDS/HP support on Mainframe to a mix of in/out-sourced IT, off-shore support structure; with an emphasis on service-based delivery.
  - ▶ Member Portals serve over 3 million users, expected to grow
  - ▶ Increased use of the SaaS, IaaS Cloud Computing Models
  - ▶ Infrastructure driven Uplift and Refresh; new CIO from Aetna
  - ▶ CISO key to driving incremental IT Security improvements

# — ABOUT Blue Shield of California

- ▶ Highly Regulated Industry
  - ▶ Healthcare Industry – HIPAA requirements (PHI)
  - ▶ Claims Processing – Financial (PII, PCI)
  - ▶ State of California – Progressive Legal Environment
- ▶ The Challenges
  - ▶ Managing our Certificates and Keys
  - ▶ Keeping the Lights On (KLO)
  - ▶ Technical Debt (Projects vs. Infrastructure & Operations)
  - ▶ Growing & Nurturing the Maturity within IT Organization
  - ▶ Increased Threats at the Edge, Insider Threat
  - ▶ Complexity of Environments, Mix of Solution Sets



# BUILDING THE BUSINESS

- ▶ Increased SSL Certificate Usage
  - ▶ Verisign Certificates used outside
  - ▶ Microsoft CA added for any inside only use
  - ▶ Partner Certificates for various projects
- ▶ Added Two-Factor Authentication for VPN access
  - ▶ Symantec VIP solution (soft token)
- ▶ Improve existing PKI assurance and processes

# BUILDING TRUST

- ▶ Build PKI with a high level of assurance
  - ▶ Secured with offline Microsoft Root and First Level CA's
  - ▶ Secured with Hardware Security Modules (HSM)
  - ▶ Secured with multi-party authentication, two-person rules



# BUILDING TRUST

- ▶ Clear, Documented Processes
- ▶ Assigned Responsibilities (Production Application Team)
- ▶ Key Management Requirements (IT Security)



# — MAINTAINING TRUST

*“You don’t know what you  
don’t know” and  
“what you think you know,  
may not really be so”  
- Unknown?*



# — MAINTAINING TRUST

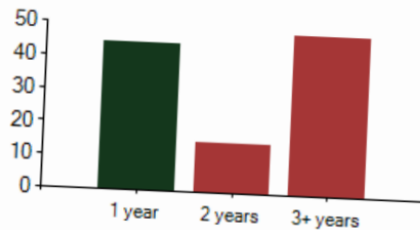
- ▶ What can break trust?
  - ▶ **Lax Management Controls**
    - ▶ Who is managing your certificates?
    - ▶ Where are the keys?
  - ▶ **Antiquated Security Standards**
    - ▶ Insecure hashing algorithms – MD5
    - ▶ Outdated Key Length (key lengths less than 1024)
    - ▶ Microsoft Patch for Internet Explorer (IE) October 2012

# MAINTAINING TRUST

## CERTIFICATE EXPIRATION REPORT



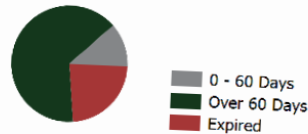
### CERTIFICATE EXPIRY



Certificates with an expiry greater than 1 year are much less secure and their use is highly discouraged.

[more info...](#)

### RENEWAL TIMEFRAME



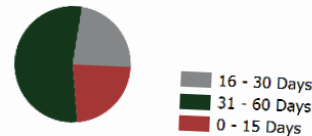
### EXPIRED CERTIFICATES

You have

**25** expired certificates. A serious security threat is to have expired certificates on the network. Currently **23.4%** of your certificates have expired.

[more info...](#)

### URGENT RENEWALS

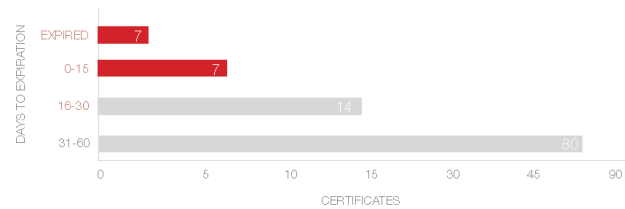


These charts provide a snapshot of when the discovered certificates expire. All expired certificates should be renewed immediately, and certificates approaching expiration should be renewed, installed, and properly configured prior to expiration.

# MAINTAINING TRUST

## EXPIRATION REPORT

Venafi Encryption Director found 104 certificates that expire in 60 days or less.

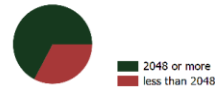


Common Name	Valid To	Contacts	Issuer	Management
license.test.nb3.np.venafi.com	9/11/2011	Admin	Entrust Certification Authority - L1C	Monitoring
license.test.nb3.np.venafi.com	9/11/2011	Admin	Entrust Certification Authority - L1C	Monitoring
license.test.nb3.np.venafi.com	9/11/2011	Admin	Entrust Certification Authority - L1C	Monitoring

## ADDITIONAL RISK AREAS



### KEY STRENGTH



NIST recommends that all certificates less than 2048 bits be removed. **32.7%** of your certificates are under 2048 bit key strength. [more info...](#)

### SIGNING ALGORITHM



NIST recognizes weaknesses in SHA-1 and recommends that all certificates should be replaced with SHA-2. [more info...](#)

### WILDCARD CERTIFICATES

Name	Hash	Count
*	985FB367C7055EB0C904D69CC93A9AF945E66550	1

▶ Suggested Free Key & Certificate Assessment

<http://www.venafi.com/products/assessor/>

# MAINTAINING TRUST

- ▶ What can break trust?
  - ▶ **Poor Key Management**
    - ▶ Expired SSL Certificates
    - ▶ Certificate CN mismatches
    - ▶ Missing policy & standards
  - ▶ **Poor Process Control**
    - ▶ Different Groups, different methods
    - ▶ Lack of Training
    - ▶ Lack of Backups for Key Experts, Contacts





# LESSONS LEARNED

- ▶ What We Really Didn't Know
  - ▶ **Things always take longer to accomplish that you think:** for example: Database Administrator (DBA) was not permitted to build the SQL Database for the Project until the Database Team had the Purchase Order (PO) in hand for the licenses.
  - ▶ **How many SSL certificates actually exist on your network:** Venafi Director revealed many more than we expected, especially the large number of self-signed SSL certificates.
  - ▶ **How many different application project teams (and third-party vendors) who have a real business need for SSL certificates:** attempting to centralize our whole process and automate the activity shall prove more challenging.

# LESSONS LEARNED

## Enterprise Key and Certificate Management Roadmap

- ▶ **Phase 1** – Getting Our Feet Wet
  - ▶ SSL Certificates
  - ▶ Policy & Standards
  - ▶ E-mail notifications
- ▶ **Phase 2** – Expanding the Pond
  - ▶ Devices
  - ▶ Other forms of certificates
- ▶ **Phase 3** – Opening the Floodgates
  - ▶ SSH Keys



# LESSONS LEARNED

## What's Next for Blue Shield of California

### ▶ **Stepping up the Game**

- ▶ Additional Training
- ▶ Moving to the latest version of the Venafi Director (v7.0)

### ▶ **Internal Education**

- ▶ Brown Bags on PKI and the Process to request certificates

### ▶ **Automate, automate, automate!**

- ▶ Policy Enforcement/Standards
- ▶ Enrollment/Renewal
- ▶ Self-Service Requests (eventually)

# LESSONS LEARNED

## What's Next for Your Organization?

### ▶ **Today**

- ▶ Do you have an internal PKI?
- ▶ What is the current state of your PKI?

### ▶ **3 Months**

- ▶ Plan for certificate based encryption and authentication.
- ▶ Develop your business case!

### ▶ **6 Months**

- ▶ Budget Money
- ▶ Budget Time
- ▶ Engage SMEs for help. If you don't get it right the first time, there can't be any trust!

