


**DATA SECURITY OVERVIEW FOR
THE CPA**

2015 New Jersey Accounting,
Business & Technology Show

May 14, 2015 / 11:00a – 11:50a

Presenter:
James C. Bourke,
CPA.CITP.CFF.CGMA

**About the
Speaker**



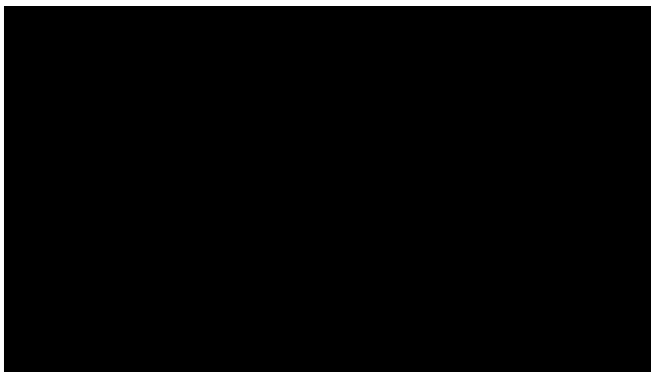
Jim Bourke
CPA.CITP.CFF.CGMA

- Partner at WithumSmith+Brown
- Responsible for overseeing all technology issues and operations for the Firm's 14 offices and over 550 employees
- Named by *Accounting Today* as one of the Top 100 Influential People in the Accounting Profession
- Named by *CPA Practice Advisor* as one of the Top 25 Thought Leaders in Public Accounting Technology
- Past President NJSCPA
- Past AICPA Board Member & Member of AICPA Council

Agenda

- **Recent Data Breach Summary**
- **2015 Predictions**
- **Best Practices to “Minimize” your Risk of Data Breach!!**











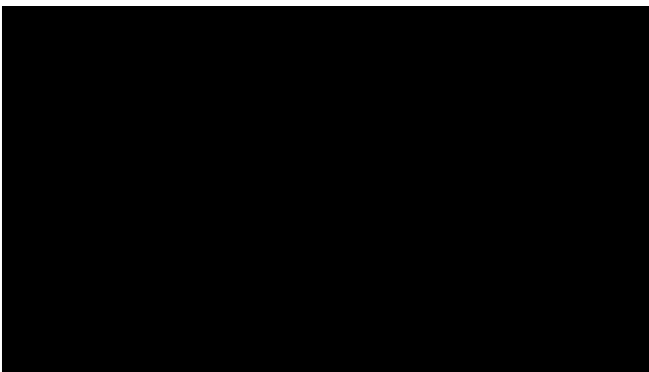














- 40 million - Credit & Debit Card Data Stolen
- 70 million - Home & Email Address Stolen
- Transactions dropped 4% post breach resulting in 46% drop in profits in Q following breach.
- March 2015 - Settlement reached to Pay Out \$10 million to victims
- CEO Terminated
- Overall Breach Related Cost estimated at >\$200 million
- \$100 million technology budget focused on securing private and confidential information
- Chip & Pin Technology for all Target Credit Cards



- 56 million - Credit & Debit Card Data Stolen
- 53 million - Email Address Stolen
- Email Addresses used in Phishing Attack disguised as a Survey offering Gift Cards
- No "evidence" that PINs were compromised - In Wake of breach, banks see spike in PIN Debit Card Fraud!
- BlackPOS - Variant - Detected by McAfee - PoSeidon new strain on POS systems
- Overall Breach Related Costs estimated at >\$65 million

WORLD WARE CHANGES UPDATED: BY [KIMPHILL](#) | COMMENTS

Start banging! World Dumps Update!



Base name: **Imperium Romanum 5**
Track 1, Track 2, State
Valid rate: 100%
No Replacements

Base name: **Imperium Romanum 4**
Track 1, Track 2, State
Valid rate: 100%
No Replacements

One of the many newer "blinger" batches added to the December Fraud Shop in recent weeks.

- Banks try to buy the batches as they are posted to look at single common point-of-purchase
- Point to Small Restaurants & Bars
- Colorado, Texas, Florida & Washington, DC area - Virginia & Maryland

VALID SHOP

Buy with Bitcoins

Cardholder Name:

Card Number:

CVV:

Country:

my card

IT'S ONLY WORK IF YOU'RE NOT HAVING A GOOD TIME.

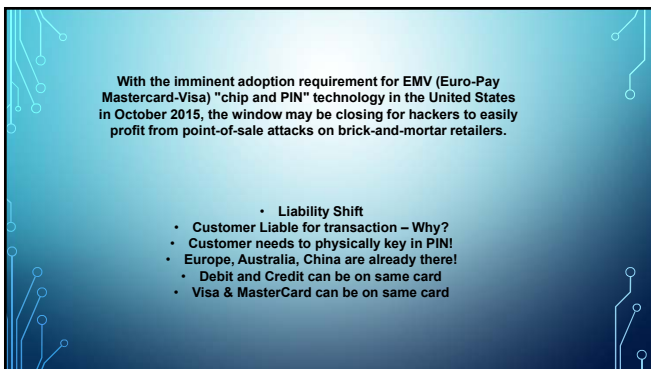
THE BOIS TUNDRA

SEE IT WORK

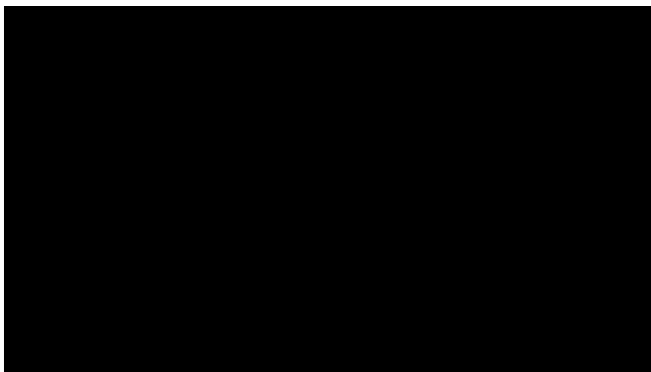
- Operates on the ".su" top-level domain (Soviet Union)
- Buy with Bitcoins
- Choose: Card, Bank Name, Country, Holder Name, Address, Phone, DOB, etc..
- "Bank of America" / "Debit Card" / "Platinum" Woman in Florida
- Cost \$4 plus 20-cent surcharge for search
- Screen with cardholder's name, card number, expiration date, CVV, full address & telephone number

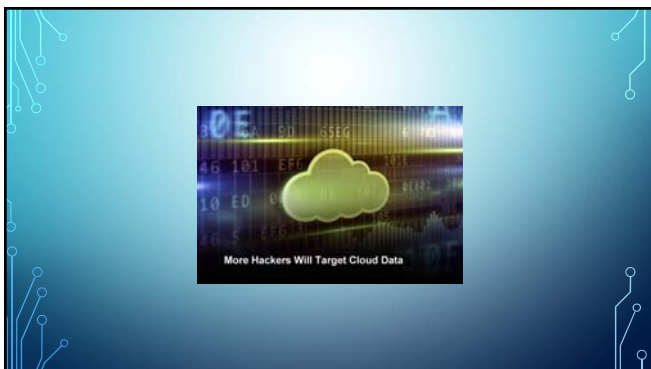




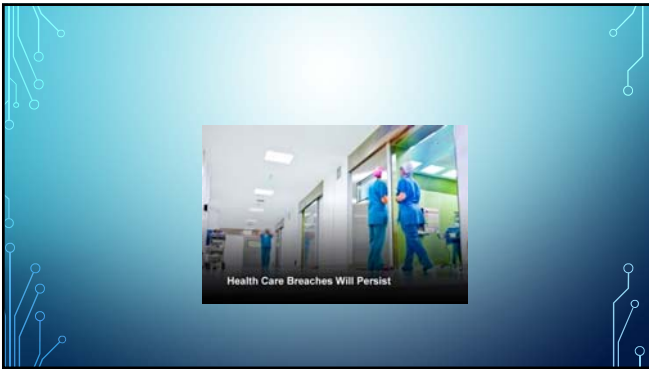








Cloud services have been beneficial to both consumers and business productivity. However, as more information gets stored in the cloud and consumers rely on online services for everything from mobile payments and banking to photo editing and commerce, they become a more attractive target for attackers. In fact, a recent study from Juniper Networks and the IBM Corporation found a Twitter account is worth more on the black market than a credit card number.



Health care breaches are expected to persist in 2015 due to multiple vulnerabilities and the high value of protected health information (PHI) on the black market. Health care organizations face the challenge of securing a significant amount of sensitive information stored on their network which, combined with the value of a medical identity string, makes them an attractive target for cyber criminals. The problem is further exasperated by the fact that many doctors' offices, clinics and hospitals may not have enough resources to safeguard their patients' PHI. In fact, an individual's Medicare card — often carried in wallets for doctors' visits — contains valuable information like a person's Social Security number (SSN) that can be used for fraud if in the wrong hands.



Where previously IT departments were responsible for explaining security incidents, cyber attacks have expanded from a tech problem to a corporate-wide issue. With this shift, business leaders are being held directly accountable for data breaches.



