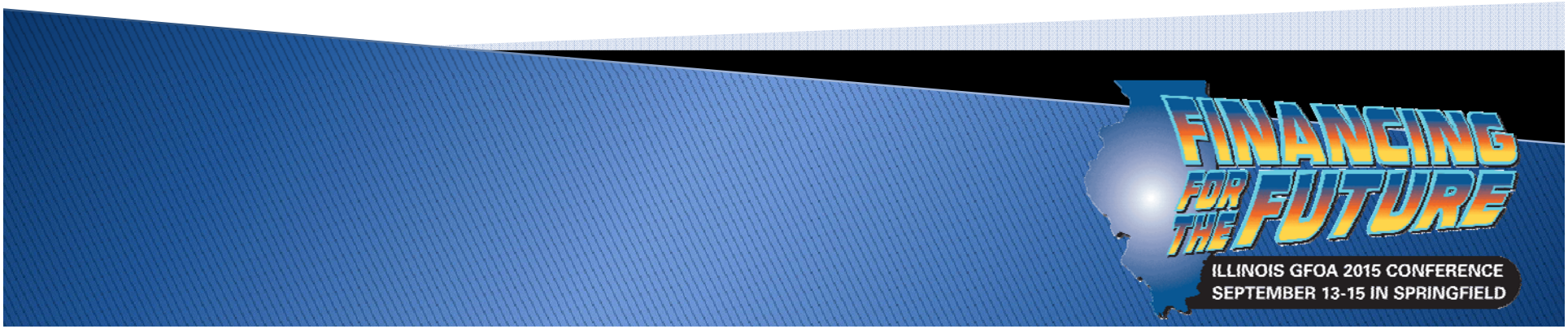
The Evolution of Data Breaches

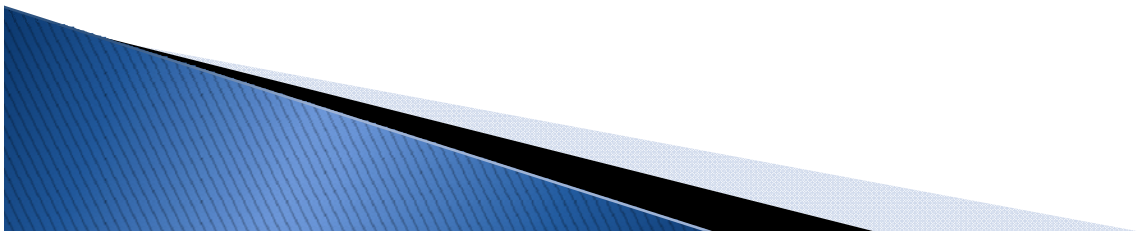
Mark Shelhart, CFI, CISSP, QSA
Security & Compliance, Sikich LLP



Retail Data Security – Recent Victims

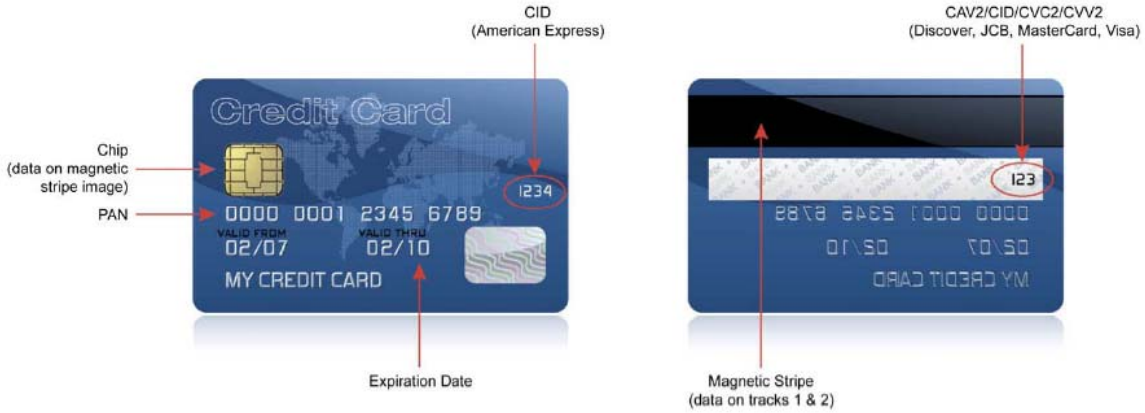
Largest Cyber Risks to Your Organization

1. Credit card breaches
2. Disgruntled IT, “bad leaver”
3. Personal records breach
4. Vendor network connections (and contracts)
5. Everything else
6. Bring your own device or “BYOD” (yes, very low on this list)
7. Lost/stolen machines



Magnetic Stripe Data

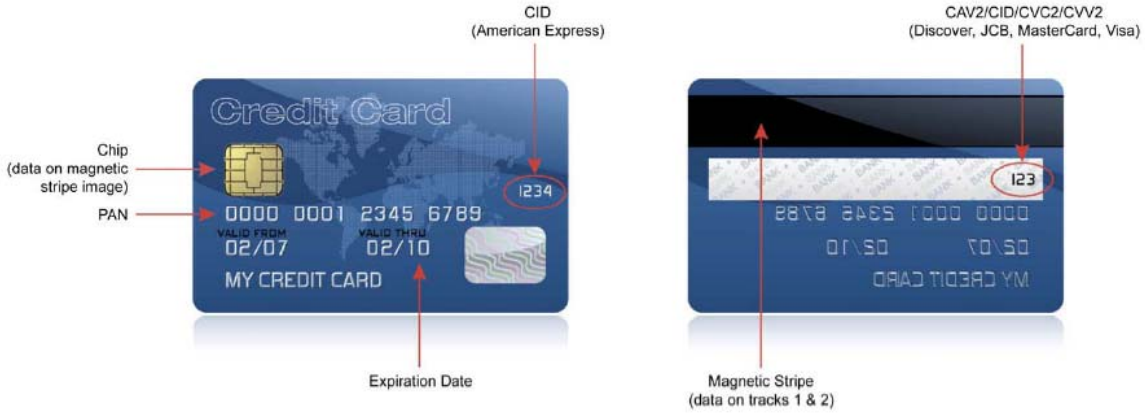
- Magnetic stripe data is the information on the BACK of a credit card
- Contains account number, name, expiration and many “hidden” digits needed to process a transaction



Track2 Captured: 82950732019230449=11102010178310003 8

Magnetic Stripe Data

- No other personal data (SSNs, street address, etc.)
- Track data is the “holy grail” for data thieves




```
Track2 Captured: 82950732019230449=11102010178310003 8
```

Flow of Most Restaurants, Stores and Hotels

FINANCING FOR THE FUTURE
ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

Card Writers on eBay

Mouse over image to zoom

Original MSR605 Magnetic Credit Card Reader Writer Magstrip Mag Strip MSR206 USB

Item condition: **New**

Quantity: 1 More than 10 available / 12 sold

Price: **US $125.00**

Buy It Now

Add to cart

Best Offer: **Make Offer**

7 watching

Add to watch list

Add to collection

Free shipping	30-day returns	New condition

Shipping: **FREE** Standard Shipping | See details
Item location: **Rosemead, California, United States**
Ships to: **United States, Canada, Europe, Australia, Mexico** See exclusions

Delivery: Estimated between **Tue. Jun. 30 and Tue. Jul. 7**
Use Expedited Shipping to get it by Jul. 2

Payments: PayPal VISA

Credit Cards processed by PayPal

PayPal CREDIT
Spend $99+ and get 6 months to pay Apply Now | See Terms

Add to watch list

Seller information
ilangsstore (476 ★)
99.2% Positive feedback

Top Rated Plus

Follow this seller

Visit store: ilangsStore
See other items

FINANCING FOR THE FUTURE
ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

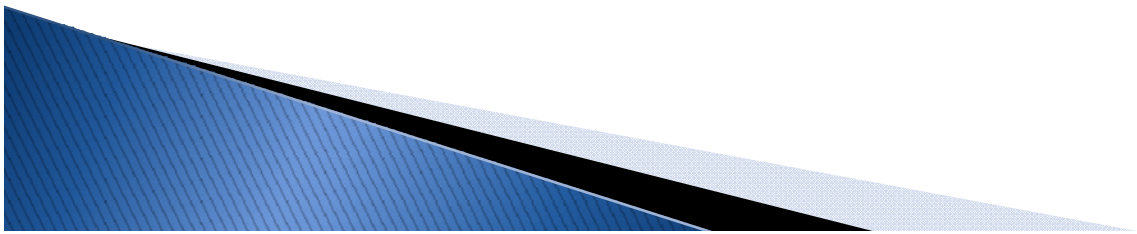
The Cost of a Breach

- The investigation
- Fines by the card brands
- Reissuance costs and fraud from issuing banks
- Regulatory penalties
- Loss of IT time
- Increased IT/audit budgets

Your Incident Response Team

- General counsel
- Information technology
  - Emotionally committed
  - Already overworked
- Outside counsel
- Public relations
- Federal law enforcement
- Executive leadership

How do YOU define the word "breach"?



The Steps

- Who found the breach?
  - Customers?
  - Law enforcement?
  - Bank?
- Containment
  - Catch the bad guy, or
  - Stop the bleeding
- Acquisition
- Analysis
- Customer notification
- Regulatory notification
- Rebuilding
  - Brand
  - Technology

FINANCING FOR THE FUTURE
ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

Cyber Attack – Factors Driving Response

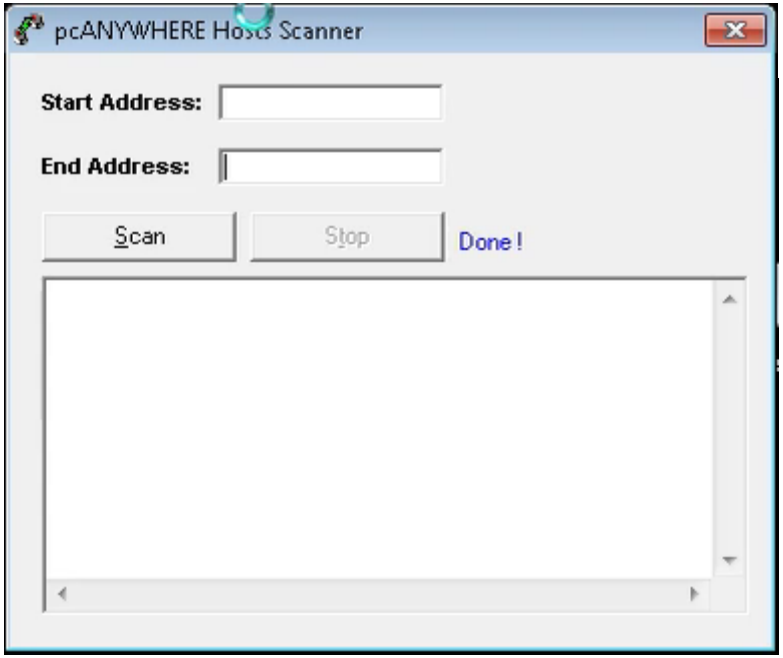
- Your investigation
  - Catch the "bad guy" versus stop the attack, versus prevent future attacks
- State laws
  - 47 states prescribe timing (30-45 days), format and content of required consumer notification
- State Attorneys General
  - 19 states require separate notices to AG
  - Focus on consumer protection
    - Varying interpretations

Hackers are Lazy

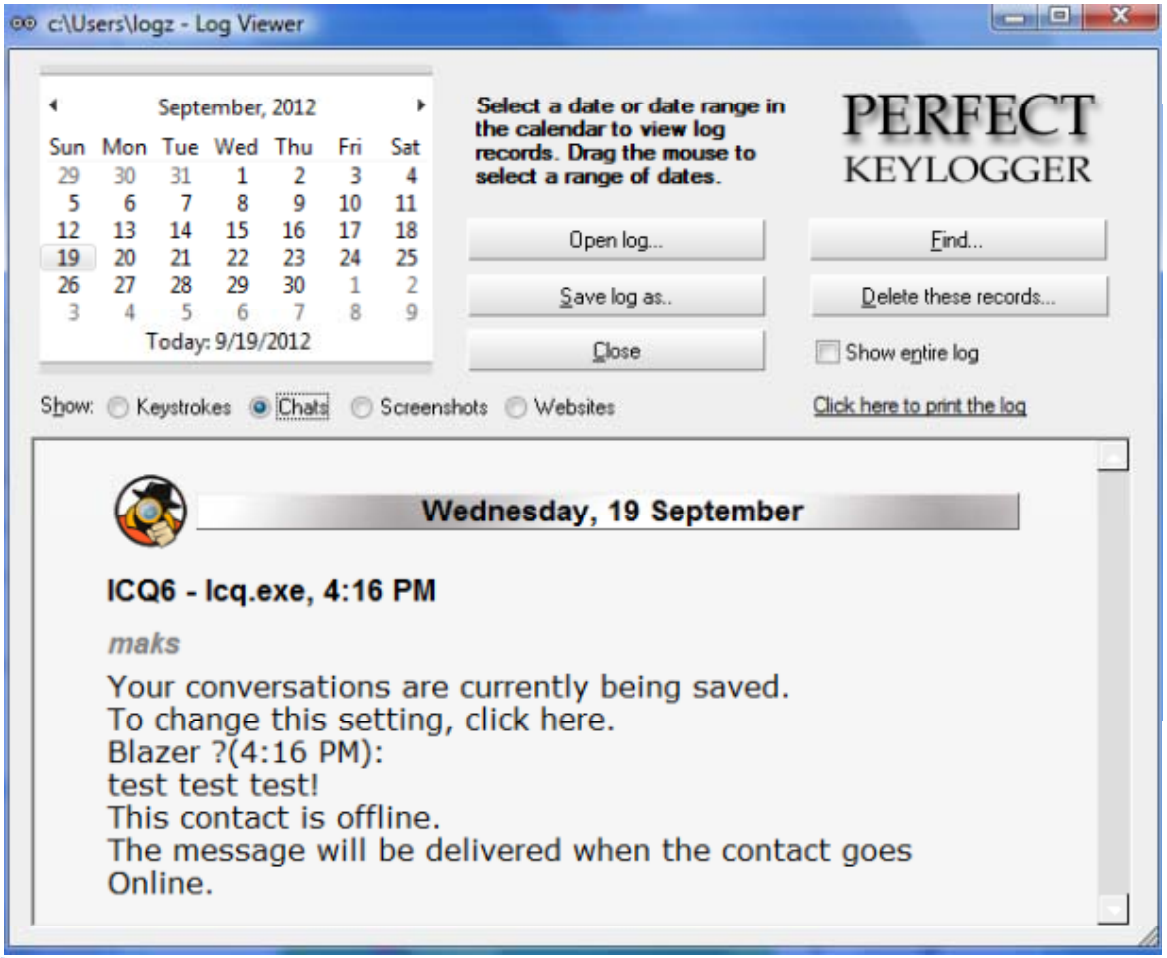
(and have been for years)

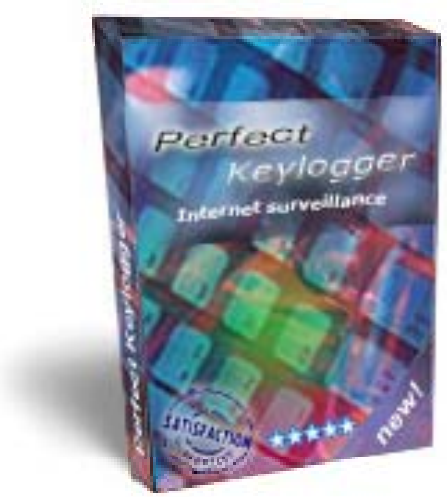
PCAnywhere Breaches (2006-2008)

- Attackers used to target major metro area
- Looking for back of house (BOH), POS, Micros…
- One laptop could scan 1 million IPs in four hours
- ~1,200 would become potential victims
- > 50 would be easy targets
- Many merchants were STORING track data
  - TJX > 90 million records



Perfect Keylogger – $29



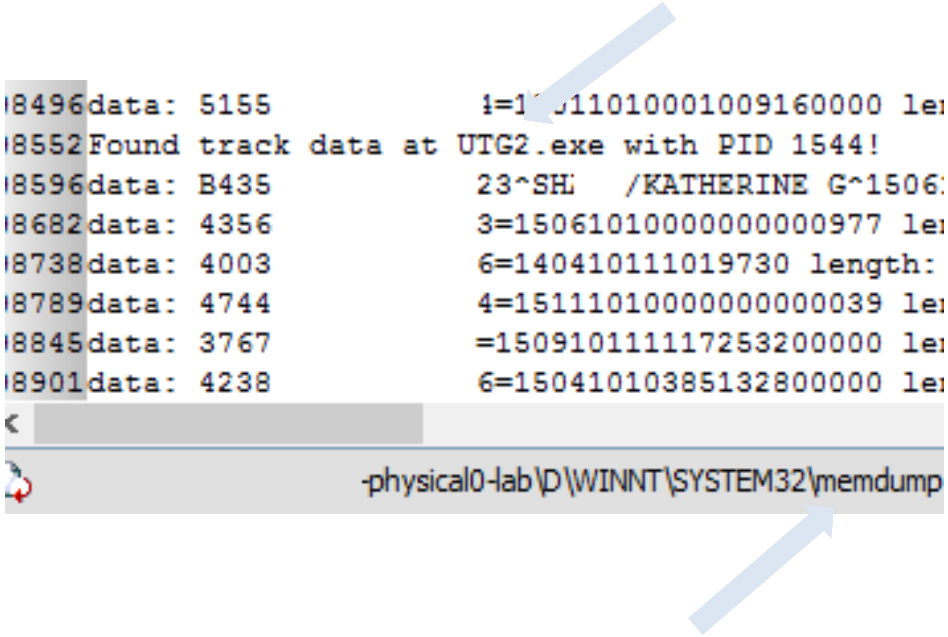


FINANCING FOR THE FUTURE
ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

Memory Dumpers – Free

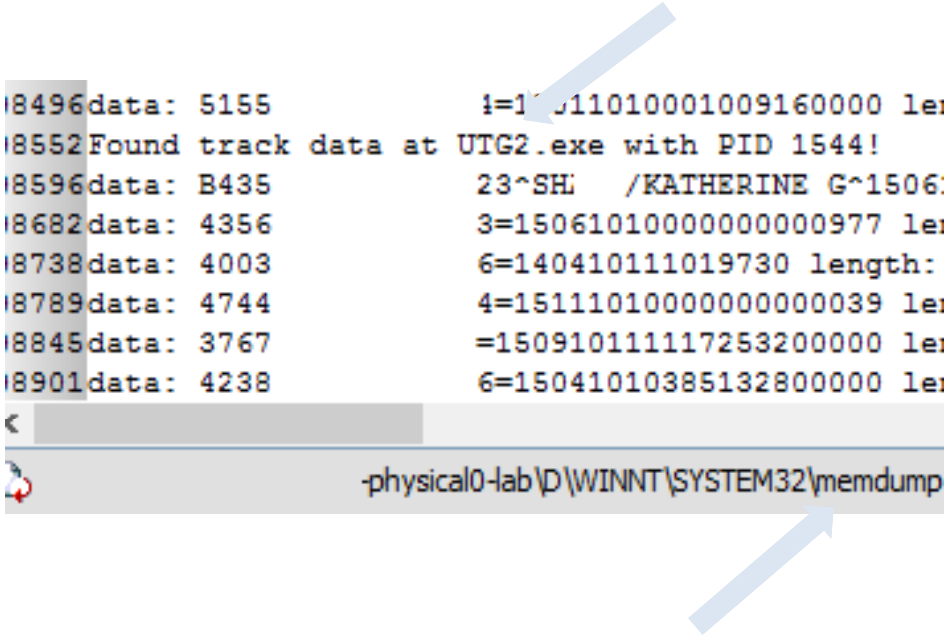
RAM Dumping Malware Targeting Tokenization

- Target: Major sporting arena
- Magnitude: This single location housed 80,000 people twice a week
- Method of entry: Remote access; no anti-virus



RAM Dumping Malware Targeting Tokenization

- Details: The attacker's malware specifically looked for programs named after popular tokenization applications
- Date range: 14 months




PASTEBIN | #1 paste tool since 2002
create new paste
PASTEBIN
Follow @pastebin
Like 200k
search
create new paste
trending pastes
sign up | login | my
Want more features
sell dumps track2; sell usa dumps; sell dumps track1;
BY: A GUEST ON NOV 3RD, 2014 | SYNTAX: NONE | SIZE: 1.79 KB | VIEWS: 155 | EXPIRES: NEVER
DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT
0
0
掌控自己的健康，
快接受乙肝檢查
點擊了解更多
CDC
1. FRESH & HOT
2. VIRGIN DUMPS;
3. T2; T12; T1+T2.
4.
5. WWW: http://vidu.su
6. ICQ: 622777999
7.
8. Hello.
9. My name is Miranda & i'm seller of dumps, T2 (T1+T2).
10. For a while I was a reseller, but then found a good team, trusted them and now i'm seller.
11. Visit my website now. While he is still working.


ViDu.Su
Fresh & Virgin
AMERICAN EXPRESS
VISA
MasterCard
DISCOVER
JUST BUY IT
ICQ: 622777999.

PCI DSS Requirements – Changing the Attacker's Approach

- Requirement 1: Install and maintain a **firewall** configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system **passwords** and other security parameters
- Requirement 3: Protect **stored** cardholder **data**
- Requirement 4: **Encrypt transmission** of cardholder data across open, public networks

PCI DSS Requirements – Changing the Attacker's Approach

- Requirement 5: Use and regularly update **anti-virus** software or programs
- Requirement 6: **Develop** and maintain secure systems and applications
- Requirement 7: **Restrict access** to cardholder data by business need-to-know
- Requirement 8: Assign a **unique ID** to each person with computer access

PCI DSS Requirements – Changing the Attacker's Approach

- Requirement 9: Restrict **physical** access to cardholder data
- Requirement 10: Track and **monitor** all access to network resources and cardholder data
- Requirement 11: Regularly **test security** systems and processes
- Requirement 12: Maintain a **policy** that addresses information security for all personnel

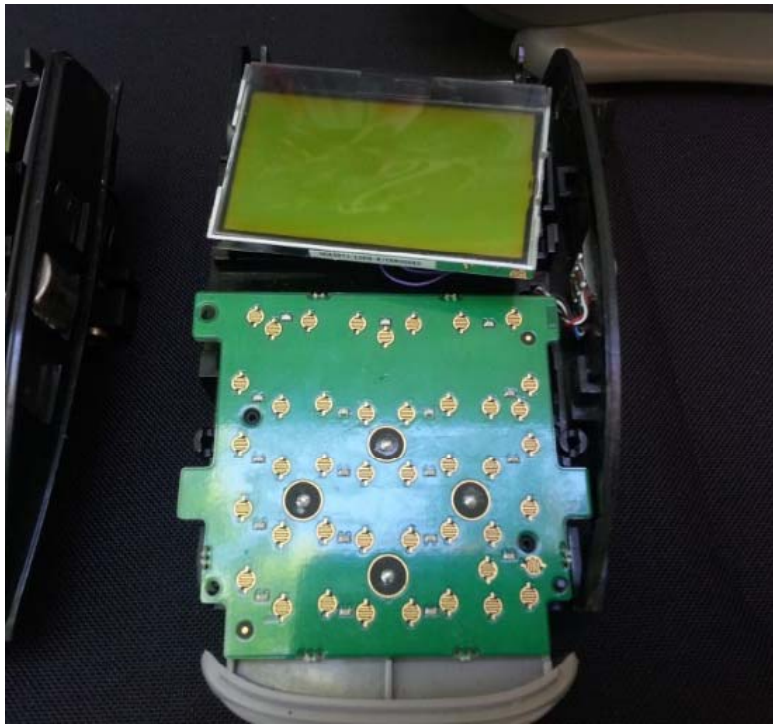
The Changing Threat Landscape

- More focused/targeted attacks based on time and effort efficiency
  - Why target thousands of IPs for random scanning if I can get data from one access point?
- Fraudulent cards are being sold based on a more targeted and geographically based approach
  - Selling by card brand, BIN and even ZIP code
- Attackers are entering the premises
  - Terminal swaps – grocery, liquor stores
  - ATM physical breach

FINANCING FOR THE FUTURE
ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

Standalone Terminals – On-Premise Hacking

- Rare but growing attack vector
- Dangerous as it also captures PIN information
- Attackers often replace the remote/desolate device
- Prevention – examine machines daily



Service Providers and Breach Trends

August 01, 2014

A wake-up call for retailers

Share this article:

Earlier this month, it was reported that Information Systems & Supplies Inc. (IS&S), a food service point-of-sale (POS) and security systems provider, notified customers of a remote access breach that may have exposed card data from POS transactions.

In a letter to customers, IS&S said a LogMeIn account used by the company to remotely support customers was breached, and they have reason to believe that the data accessed could include credit card information.

The article notes, "IS&S is an independent reseller of POS products sold by software vendor Future POS Inc. Future POS customers named on IS&S's site include restaurant chains such as Dairy Queen and TacoTime."

The POS vendor's president went on to confirm that his company's remote access credentials were compromised, possibly through a phishing attack.

Boatner Blankenstein, senior director of solutions engineering, Bomgar Corporation

While IS&S should be commended for immediately notifying customers about the potential breach and also taking steps to improve remote access security, this breach is yet another wake-up call for retail and hospitality chains to evaluate their third-party vendors.

The circumstances of this event are similar to the massive Target data breach that occurred late last year, in which hackers compromised an HVAC vendors' credentials to initially infiltrate the big box retailer's network.

Vendor-Related Risk

- Vendor remote access
- Vendor servers on network
  - Often IT does not have control
  - No anti-virus, not patched, weak passwords
- Vendor on network with BYOD
- Vendors without incident response details in their contract

LogMeIn – 2014

- Resellers and integrators are the Achilles heel of POS users
- 100–1,000 businesses can be breached in a matter of hours
- Resellers often make quasi-strong passwords
  - Attackers quickly figure these out

FINANCING FOR THE FUTURE
ILLINOIS GFOA 2015 CONFERENCE
SEPTEMBER 13-15 IN SPRINGFIELD

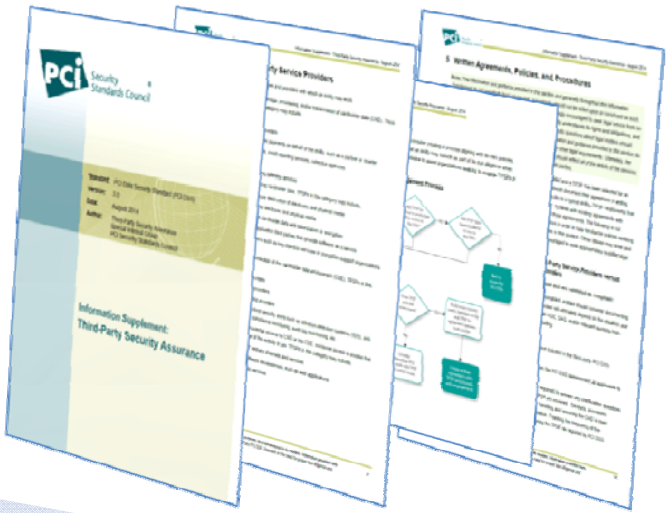
LogMeIn – 2014

- Backoff also has some direct correlation to phishing attacks
- Attackers are phishing IT people to gain LogMeIn credentials
  - IT people are smart, but often busy
  - IT people often don't apply the same security to their own PCs

Third Party Security Assurance

Main areas of focus:

- Third-party service provider due diligence
- Service correlation to PCI DSS requirements
- Written agreements and policies/procedures
- Monitoring service provider compliance status



What About Breach Protection?

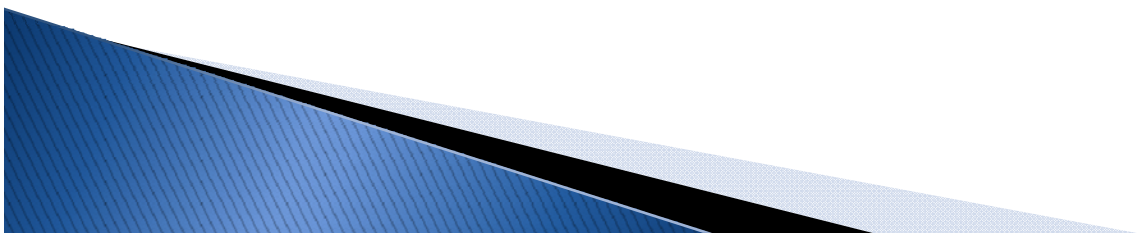
- Typically covers up to $50k or $100k
  - Forensic investigation
  - Fines and penalties
  - Card replacement costs
  - Some plans cover POS system upgrades
- Makes the post-breach process better all around
  - For the merchant – Allows things to move faster/easier to work with
  - For the acquirer – Knows they will not be left holding the bag on all the possible costs

What About Cyber Insurance?

- Cyber insurance typically covers:
  - Forensic investigation (overlap with breach protection)
  - Should include first party and third party activities
  - Crisis management costs – notifications, etc.
  - May include coverage of consumer civil suits relating to identity theft

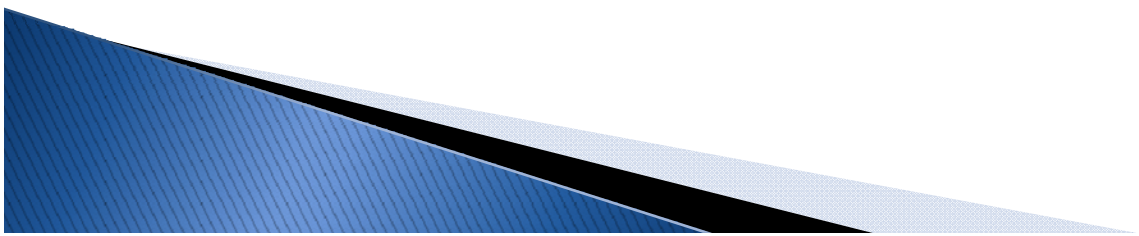
What Could Have Stopped These Breaches?

- Securing remote access ('14 & '15 breaches)
  - Must be turned on by a human at the store locations
  - Two-factor authentication
  - Management, not just IT, should get notification when someone is working on the critical systems
- Firewalls that block outbound connectivity
  - Your board should understand what "whitelisting" means
  - Corporations (and firewall vendors) should not let merchants opt out



What Could Have Stopped These Breaches?

- Segmentation
  - Corporate networks and guest wireless should be separate from critical systems
  - Site-to-site communication should be forbidden, even for IT functions

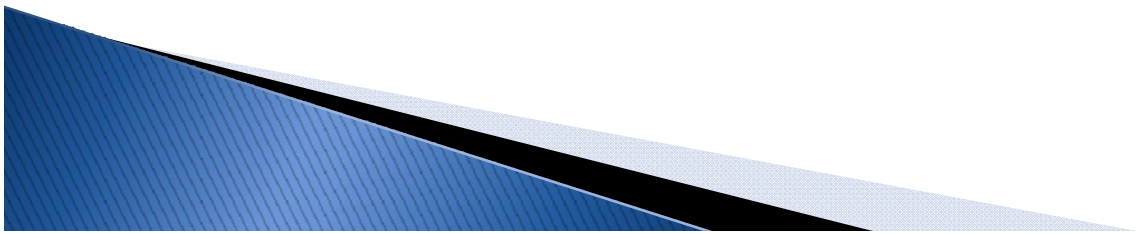


Network Scope & Segmentation

- PCI or otherwise
  - TJX (2006)
  - Target (2013)
- Reduce your liability
- This includes infrastructure
  - Patching server in Office A should not reach Office B

What Your Organization Must Change (Right Now)

- Block outbound connectivity – whitelist, not blacklist for critical infrastructure
- Segmentation
  - Users (and servers) in Office A should not be able to access Office B
- Remote access
  - Control it, MONITOR it
    - 11:00 p.m. remote access is no different than an employee in the office at 11:00 p.m.
  - Two-factor authentication, no exceptions



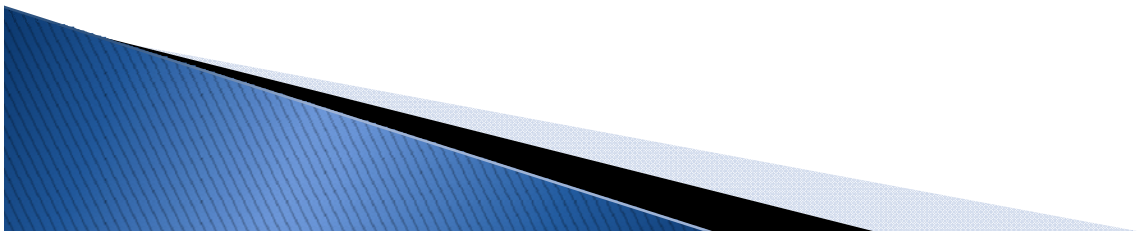
What Your Organization Must Change (Right Now)

- Service accounts (or any unchanged passwords)
- Integrate humans into security monitoring
- Vendors
  - Fix contracts to allow audits and investigations
  - Vendors also include “the cloud”

Looking Forward

If the last 30 minutes did not scare you:

- Corporate espionage
  - Would your competitors want to know your success methods, your budget?
  - Domestic or foreign
- Road warrior dangers
- Tradeshow spying



Questions?

Mark Shelhart, CFI, CISSP, QSA
Sikich LLP
mshelhart@sikich.com
www.sikich.com
877.403.5227 x221