AASHTO IS 2012
MAY 14TH - 17TH
TRArVERSE CITY

Modernizing Transportation with Technology
CYBERSECURITY: Your Future, Your Cloud, Your Smartphone

Dan Lohrmann, Michigan Chief Security Officer
May 16, 2012
What’s on Tap for Today?

- Changing Technology, Changing Challenges
- Three Things that Keep Me Up at Night
- Cloud Technology
- Mobile Technology
- The User Awareness Challenge
- What We Can Do
Where We Were
Where We Are
Where We’re Headed
Let the Robot Drive . . .

WIRED Magazine – February 2012
A New Target?

As systems and products become more technology-reliant, the hackers move their sights.

Hackers to target and cyberattack high tech cars?

Forget about hackers targeting smartphones or your home computer because "hackers have scopes set on your automobile," according to The Montreal Gazette. From a lab, security researchers were able to "send nasty messages to their test car’s display board, start and stop the engine, disable the brakes and even make two cars 1,000 miles apart perform in unison. Could any basement-dwelling computer geek do the same thing?"

Some security researchers warn that any electronic system in a car is a potential target for hackers, from the brakes to the radio. In fact there are all kinds of sweet spot automotive attack surfaces. We are incorporating more entertainment-related computers in cars, entertainment systems that can be hacked to tell safety computers what to do. Yet we continue forward so
Die Hard 4 – Fact or Fiction?
What Keeps Us Up at Night?

Give me YOUR list . . .

At each table – identify a Spokesperson and:

1. Each person identify one cyber issue that keeps you awake – and why?
2. Time permitting – do it again.
3. Select no more than 3 issues to report out to the wider group.
Dan’s Top Three

#1 – Securing the Cloud

Pro:
- Cost Savings
- Ease of Migration

Con:
- New Technology
- Untested
- Compliance Challenges
Dan’s Top Three

#2 – Bring Your Own Device (Or not . . . )
Intel predicts that by 2016:

• 80% of organizations will be utilizing the Cloud
• 80% of workforce will be using their own personal devices for work (BYOD)
Dan’s Top Three

#3 – Training and Awareness Education for Users

Current model is
- Boring
- Outdated
- Audit Exercise
- Not Required
## Engaging Security

### Business
- Clearly articulates business need to security team.
- Listens to security risks, makes **informed** decisions.
- Works **with** the security team to securely accomplish business goal.

### Security Team
- Learns business need and develops SECURE solutions.
- Provides options – Gold, Silver, Bronze – identifying risks/costs.
- Works **with** the business to securely accomplish business goal.
“8 Core Beliefs of Extraordinary Bosses”

#1: Business is an ecosystem, not a battlefield.
#2: A company is a community, not a machine.
#3: Management is service, not control.
#4: My employees are my peers, not my children.
#5: Motivation comes from vision, not from fear.
#6: Change equals growth, not pain.
#7: Technology offers empowerment, not automation.
#8: Work should be fun, not mere toil.

Source: Geoffrey James, Inc. Magazine April 23, 2012
Another Table Discussion

• Is your IT security organization . . .
  ■ Providing options, or using a one-size-fits-all approach?
  ■ The first, or last, to find out about new implementations?
  ■ Invited to the table up-front, or avoided?
  ■ A trusted partner for your business, or a viewed as the party-pooper?

• Complete this sentence: If I could change one thing about our security organization, it would be ________.
Let’s Look Closer . . .

• Cloud Computing –
  ■ Get Ready!

• Bring Your Own Device (BYOD)
  ■ The Good, The Bad, and The Ugly

• Security Awareness Training –
  ■ What Works, and What Doesn’t?
A Closer Look . . . Cloud

Manage primary and secondary functions through a strategic tiered approach based on the criticality of the function.
It’s Coming . . . It’s Here . . . Cloud

- Prepare for the Trend
- Public/Private Clouds
- FedRAMP 2013
  - Initiate
  - Assess
  - Authorize
  - Leverage

Get ready for the everything-as-a-service world

By Steve Charles  ■ Apr 12, 2012

You might not have Eucalyptus bookmarked. But if you plan on selling software and software services to the federal government, it’s the kind of thing with which you need to become familiar. What is it? Eucalyptus is open-source software that lets developers use industry standard application programming interfaces to build private clouds or hybrid clouds that draw from internal and external, or public, cloud resources.

Why is this important to federal technology marketers? Because it’s emblematic of an important technology trend in the government that will start to gather momentum later this year and into fiscal 2013. Namely, for want of...
Michigan’s Cloud

External clouds may not be a viable option for every function, particularly those that have very sensitive data or have a security requirement. Michigan will continue to securely house such functions in its government cloud.

Examples:
- Health Records
- Taxes
- Criminal justice Data
Secondary Clouds - External

Key targets for external clouds are vast and provide exciting opportunities for the delivery of non-critical functions.

Examples:
Human Resources
e-Mail
Messaging

When it comes to managing external clouds, there are two extremes . . .
Securing the Cloud

One extreme  

BLIND TRUST:  
• Adopt a commodity cloud function as-is (cloud sets the rules)  
• BUT: Provider accountability is low while risks are high

To the other  

CONTROL:  
• Dictate the standards, terms & conditions, etc.  
• BUT: No longer an as-is commodity (and no longer cheap!)
The Middle Road

It’s our job to find the right balance by setting some **basic parameters** for external cloud computing…

- Ownership
- Security
- Legal issues (privacy)
- Location for hosting
- SLAs

This gives us the best of both worlds in terms of **reduced costs, accountability and agility**
Getting Started . . .

How do you determine which applications are appropriate for the cloud, and which are not?

- Understand your application portfolio
- Understand application compliance requirements
- Understand your risk

Can cloud services alone be trusted with your critical applications and data?

The answer is simple: trust, but VERIFY.
Bottom Line . . .

• Develop a strong implementation strategy!
• Enforce password and log-in controls!
• Make your users aware of their responsibilities!
• Track your assets – know what’s on your network!
A Closer Look . . . BYOD

The Good -
- Cost Effective
- Convenient
- Increased Productivity

Study: Personal devices now used for work in 88% of businesses

Corporate Applications and Services Used on Employee Personal Devices

- Email: 85%
- Social Networking: 46%
- Customer Relationship Management: 45%
- Time and Expense Tracking: 44%
- Enterprise Resource Planning: 38%
A Closer Look . . . BYOD

The Bad -

- Hard to Secure
- Easy to Lose
- Hacker Target

Breach Of The Week: Your Smartphone Is A Hacker Paradise

BY KIT EATON | 07-29-2011 | 9:03 AM

Packed with personal data, and taken with you everywhere, your smartphone is...
A Closer Look . . . BYOD

The Ugly . . .
The Dreaded “B” Word – BREACH

Tech Insight: Smartphones The New Lost And Stolen Laptops Of Data Breaches

Mobile device management and a new spin on user awareness training are essential to the enterprise mobile explosion

Oct 07, 2011 | 02:52 PM |

By John H. Sawyer
Dark Reading

Enterprises have enacted full-disk encryption to protect themselves from their data being exposed through careless users. And the same trustworthy users who’ve left laptops in taxis or had them stolen from the local coffee shop are now forcing companies to deal with mobile devices that are smaller, always-on, unmanaged, and need to be plugged into the corporate network.

Management and IT are butting heads on the issue. Why? The trend of users to bring in personal devices might be saving money when a
The Mobile Wallet

• 38% of Users make purchases with their smartphone device
• 21% of Users do their banking with their smartphone device
• Trending upward – most users expected to use mobile wallet by 2020

Source: Pew Internet Survey 2012
BYOD – A Secure Approach

- Access Controls
- Remote Wiping
- Encryption
- Password Policy
- Firewall Protection
- Content Management
- Data Classification
- User Training

Securing Smartphones for Government Use

SPECIAL REPORT: Smartphones & PDAs

By Barbara DePompa, 1105 Government Information Group Custom Media

As the use of smartphones and PDAs in the federal government continues to grow, so do the security risks, which range from loss or theft of devices to malware infections, text, voice or email spam (used for phishing), to electronic eavesdropping, location tracking, theft of service through cloning and exposure of sensitive data at the server.

Via a range of specialized features such as cameras, Global Positioning System navigation, removable-media card slots and wireless interfaces that include infrared, WiFi, Bluetooth, as well as multiple cellular interfaces, these handheld devices can introduce a variety of vulnerabilities that federal agencies must somehow address.
Bottom Line . . .

• Evaluate your business portfolio!
• Classify your data and determine ownership!
• Engage your security team up front – they can help!
Back to You . . .

• What are you currently doing with Cloud?
• How are you securing Smartphones?
• Do you allow employees to BYOD?
• Is it working?
A Closer Look . . . Awareness

Current Pitfalls:

- One-size-fits-all, irrelevant.
- Boring, “Death by PowerPoint.”
- Outdated materials, stale content.
- “Check the Box” exercise.
- User thinks security is “someone else’s job.”
- Audit/compliance oriented.

So, what’s the solution?
A Quick Quiz . . .

Question: What percent of breaches are the result of user error?

25%
45%
59%

According to CompTIA study, 96% of those surveyed would now recommend user training.
How Have We Addressed It?

“PIC” – Problem in Chair
The Right Approach

• Give employees the “carrot” and award a certificate . . .

• Or bring out the “stick” and deny access?

Answer: A combination of both!
Cyber Awareness Training 2.0

Make the training sessions . . .
- Intriguing
- Relevant
- Fun
- Focused
- Clear and easy to understand
- Effective

Modernizing Transportation with Technology
Fun Training?

Where is the #1 location for lost devices at the airport?

- Security Checkpoint
- Restroom
- VIP Lounge
- Food Court
- None of the above
Bottom Line

• Engage your users – make training content relevant to their lives, home AND work!
• Keep your training current!
• Make it fun!
• Keep it clear and concise!
Final Thoughts . . .

• As technology evolves, so must the business. Today’s security problems are NOT the security problems of tomorrow!

• Your users are your greatest asset, and your greatest liability – effective awareness training will create a trusted partnership and protect your business!

• Make informed decisions and seek out your security team – they really DO want to help!
Questions?

Daniel J. Lohrmann, Michigan Chief Security Officer
Phone: 517-241-4090
LohrmannD@michigan.gov
Michigan Cyber Website: www.michigan.gov/cybersecurity