

Hacking: Its Implications on the Electronic Mortgage Process

Chuck Herrin, United Guaranty Corp.

Jon Fox, Freddie Mac

Yuriy Dzambasow, A&N Associates, Inc.

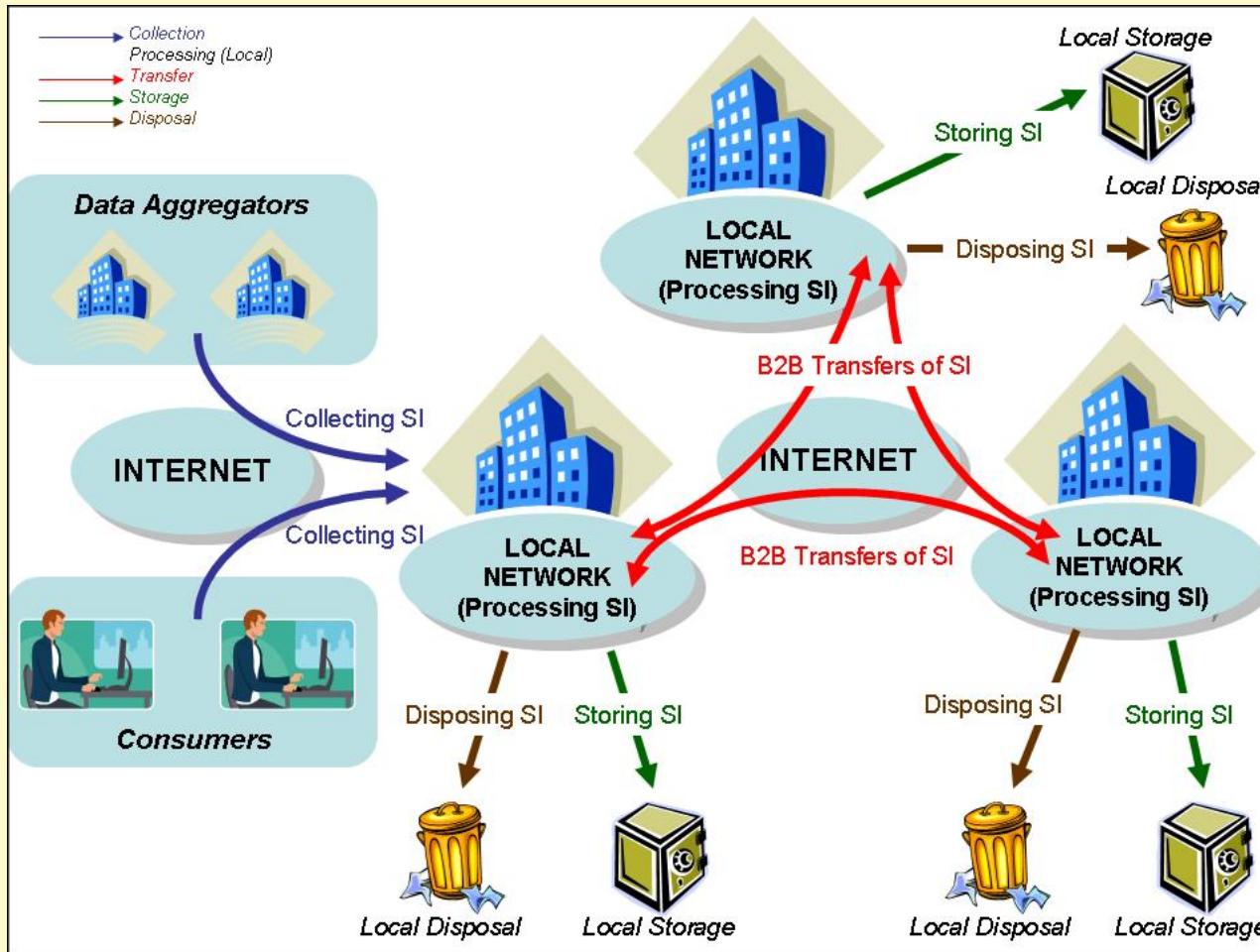
March 30, 2006

- Agenda:
 - » Critical use cases for handling sensitive information
 - » Common hacking techniques
 - » Examples of real-world hacking
 - » Suggestions for your organization
- Format:
 - » Discuss (mostly Yuriy)
 - » Demonstrate (mostly Chuck)
 - » Suggest (mostly Jon)

- Sensitive Information (SI) permeates electronic mortgage processes
- Understanding where SI exists in your organizational workflows helps identify what hacking threats to worry about
- Most hacking can be done very quickly
- Hacking is just not “traditional network hacking”
- Hacking happens to every type of organization
- There are practices your organization can embrace to better protect from hacking SI



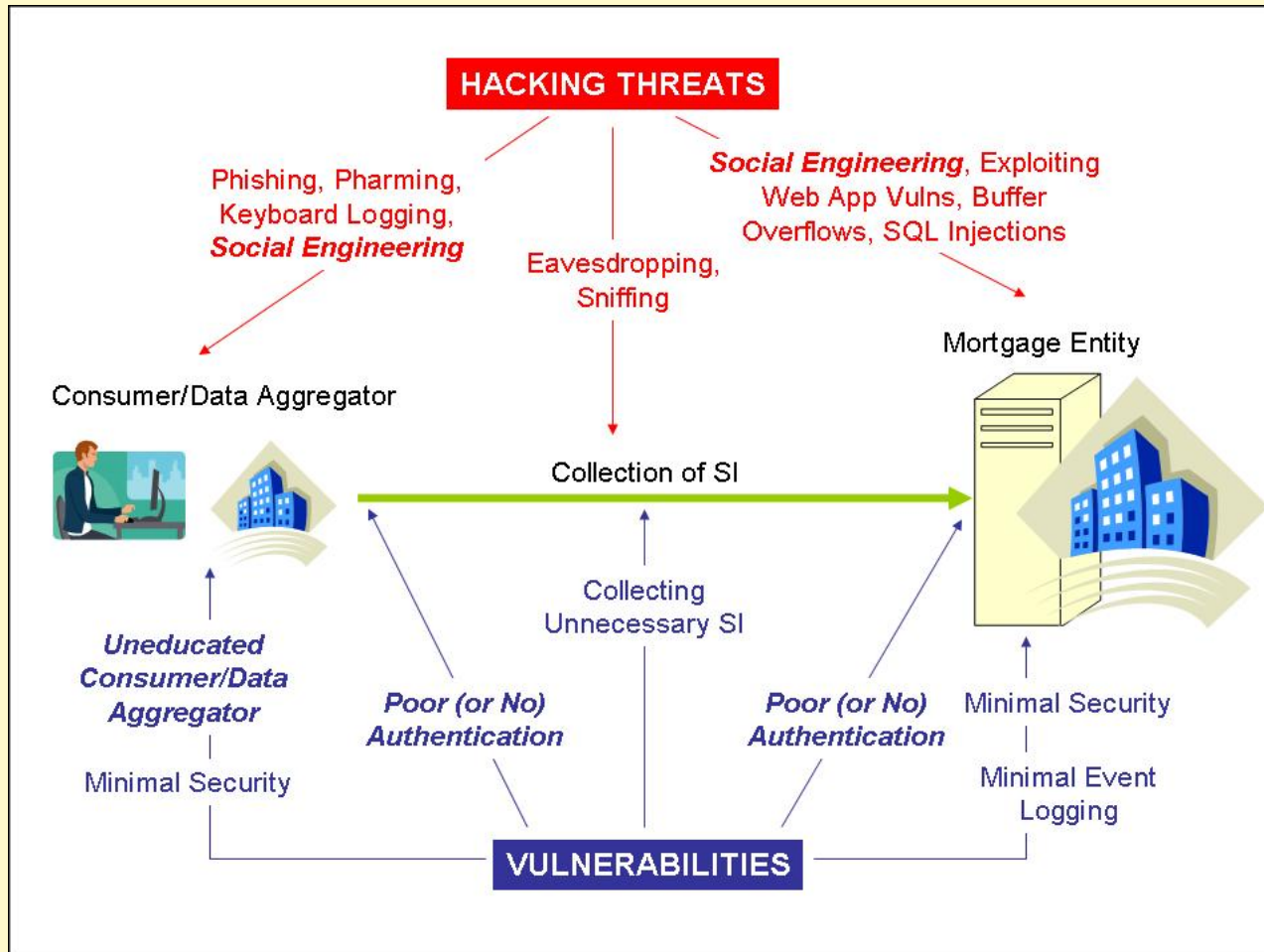
Sensitive Information (SI) Use Cases



- Collection
- Processing
- Transfer
- Storage
- Disposal



- **Collection**
the initial gathering of personal information from a consumer to support an electronic mortgage function or process
- **Processing**
an organization's internal use of sensitive information, by their employees or computing environment, to execute an electronic mortgage workflow activity (e.g., loan processing)
- **Transferring**
the sending and receiving of sensitive information between two mortgage entities
- **Storing**
the placement of sensitive information into either temporary or long term containers
- **Disposing**
the deletion or discarding of sensitive information that is no longer needed within an electronic mortgage process or function



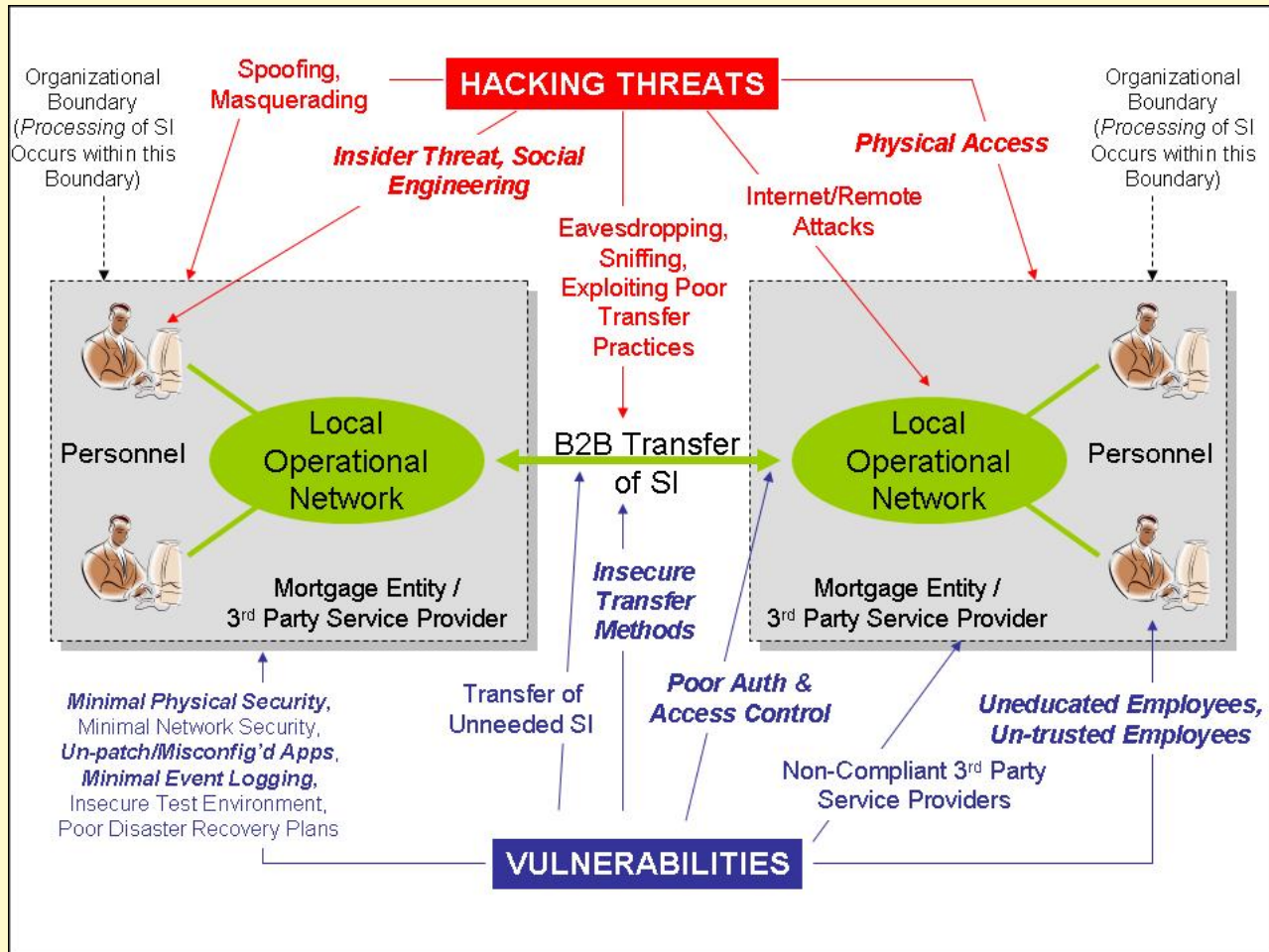


DEMONSTRATION:

How would your employees respond to a call like this?

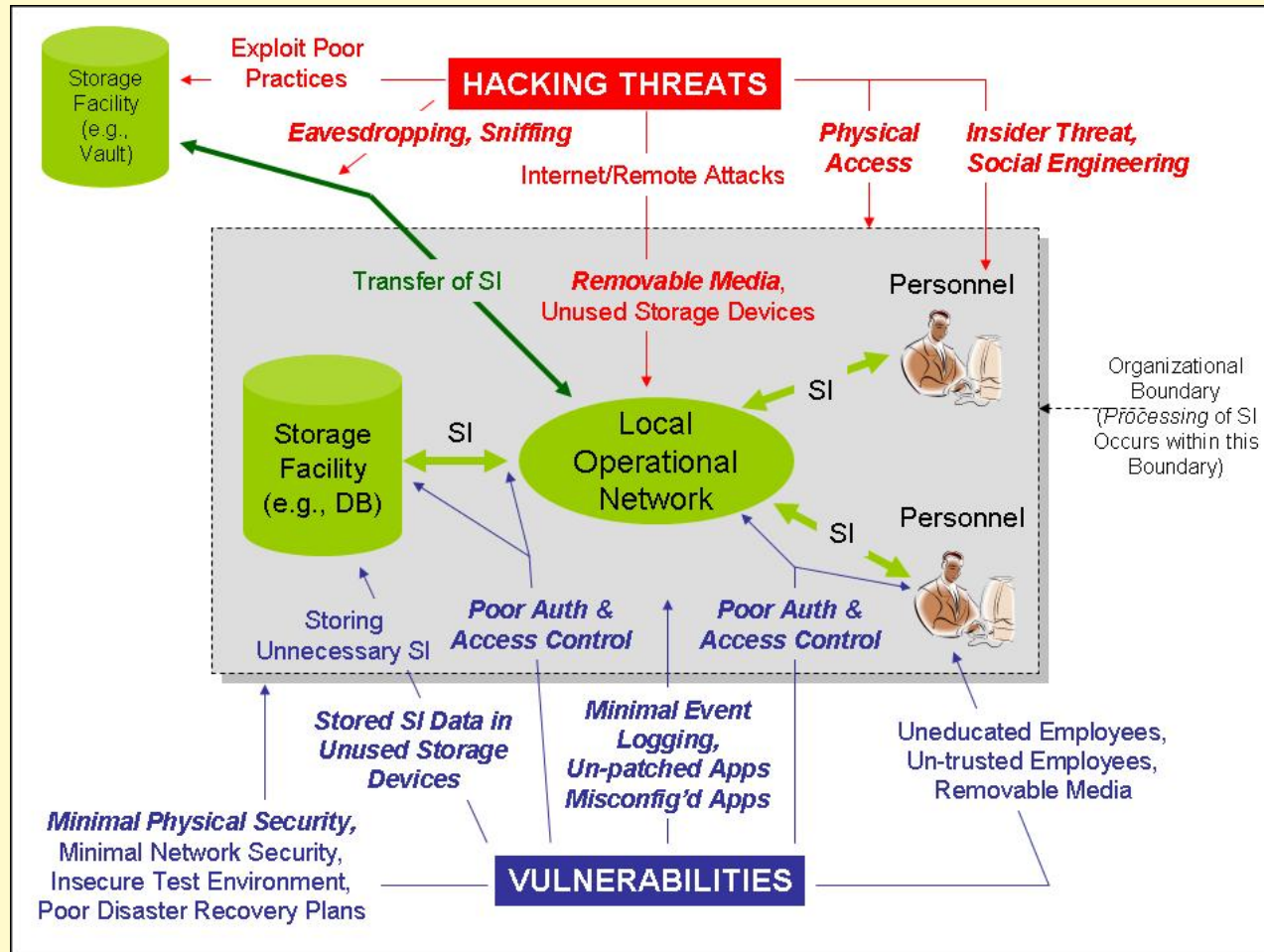


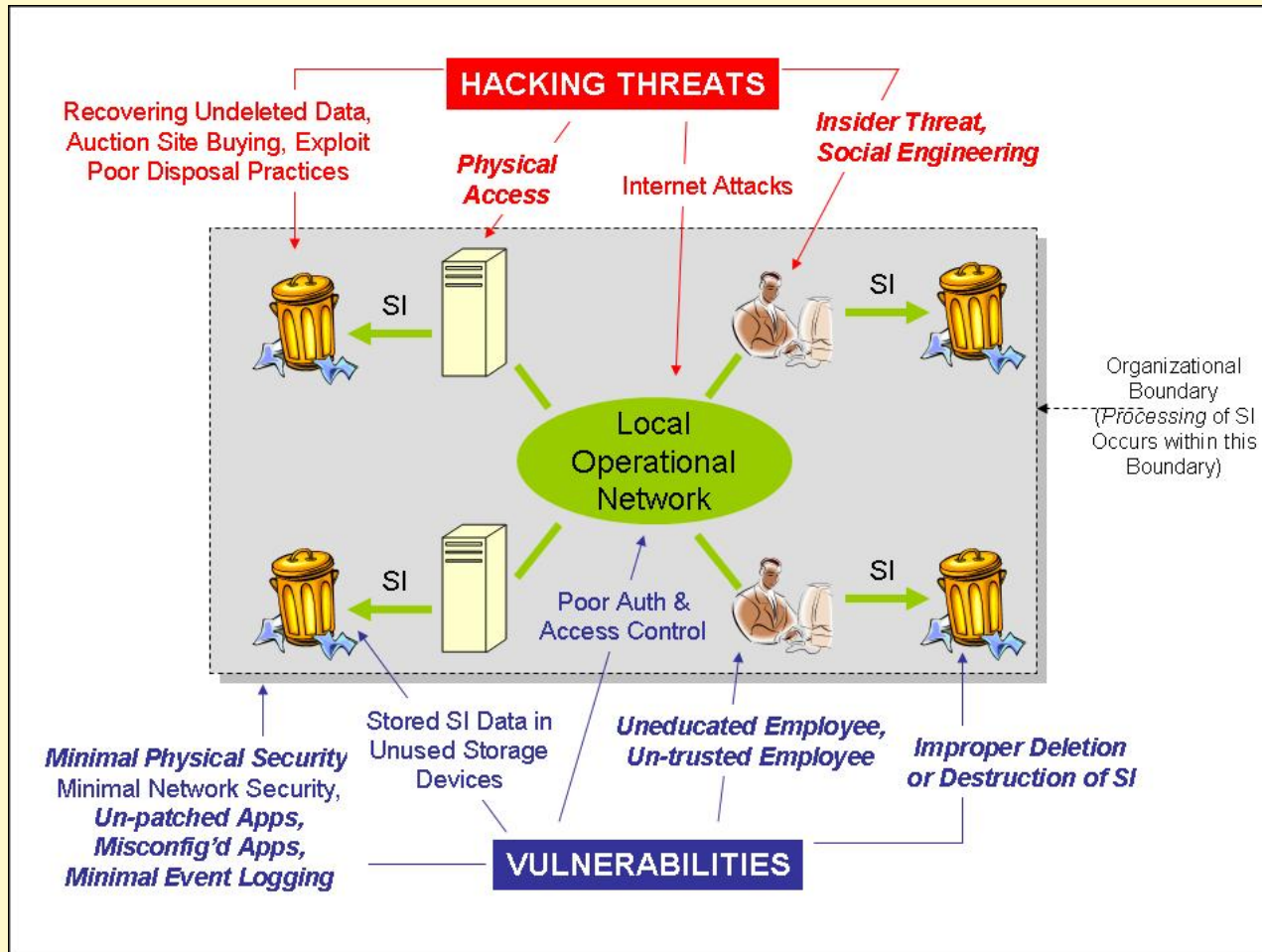
DEMONSTRATION: Web Servers – Your Business' Gateway to the World.





DEMONSTRATION: Physical Access Trumps Everything!

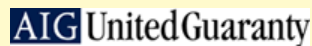






DEMONSTRATION:
Excel – Truly a Powerful Tool...
But For Whom?

Company Type*	Event Type	No. or People Affected	Estimated Financial Impact**
Data Aggregator	Social Engineering	162K	\$22.68M
Financial Institution	Lost Backup Tapes	1.2M	\$168M
Data Aggregator	Compromised Passwords	312K	\$43.68
Data Processor	Network Hacking	40M	\$5.6B
Retailer	Network Hacking	1.4M	\$196M
Higher Education	Stolen Laptop	98.4K	\$13.78M
Higher Education	Dishonest Insider	150K	\$21M
Financial Institutions (Multiple)	Dishonest Insiders	676K	\$94.64M
Media Firm	Lost Backup Tapes	600K	\$84M
Media Firms (Multiple)	Data Exposure	240K	\$33.6M
DMV	Dishonest Insider	465K	\$65.1M



* Info obtained from <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

** Estimate is based on PGP Research Report Study – November 2005

- Get Senior Management buy-in to prioritize and fund a comprehensive security program within your organization
- Identify leadership and responsibility for the security program
- Establish credibility with your security program/team
- Understand the SI use cases that apply to your organization
- Ensure your security program addresses five fundamental areas:
 - » Business analysis, asset identification, and risk assessment
 - » **Security policy** and architecture
 - » Security specifications (people, processes and technologies)
 - » Security monitoring and maintenance
 - » **Security awareness and education**



- Create a cross-functional security steering committee (business areas and IT)
- Establish and maintain an active communication channel between security, privacy, and legal/regulatory affairs offices
- Establish a cadre of penetration testing vendors, schedule and execute tests for perimeter, infrastructure, and key applications
- Adopt an information security program framework (e.g., ISO17799/ISO27001)
- Benchmark your information security program on a regular basis (e.g., every 24 months)



- Stay abreast of security trends (including hacking trends):
 - » Hackers will pursue new avenues when old ones are exhausted
 - » Vulnerabilities, exploits, technologies and techniques change frequently
- Familiarize yourself with resources such as:
 - » SANS Institute Top 20 (<http://www.sans.org/top20/>)
 - » Bugtraq (<http://www.securityfocus.com/archive/1>)
 - » CERT Coordination Center (<http://www.cert.org/>)
 - » Financial Services Information Sharing and Analysis Center (<http://www.fsisac.com>)
 - » Vendor Specific sites (e.g., Microsoft, CISCO)
- Attend security conferences and workshops (e.g., RSA, CSI, DEFCON)
- Follow the activities and work products of the MISMO Information Security Working Group (ISWG) at <https://sharepoint.mismo.org>



Chuck Herrin

Director of Information Security
United Guaranty Corp.

336-333-0567

herrinc@ugcorp.com

www.ugcorp.com

Yuriy Dzambasow

Principal Consultant
A&N Associates, Inc.

410-859-5449 x107

yuriy@anassoc.com

www.anassoc.com

Jon Fox

Vice President – Information Security &
Technology Change Management

Freddie Mac

703-714-3900

jon_fox@freddiemac.com

www.freddiemac.com

RJ Schlecht

Director – Industry Technology and Security
Compliance

Mortgage Bankers Association

202-557-2843

rschlecht@mortgagebankers.org

www.mortgagebankers.org