

Session BOF 7

PII and Security

Bridget-Anne Hampden
U.S. Department of Education



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Guaranty Agency Reviews

Why We Did It...

How We Did It...

What We Did...

What We Found...

Next Steps...



Why We Did It... (Background)

- PII Breach reported in March 2010
- 2010 Guaranty Agency (GA) Security and Privacy Conference in Washington, DC
- Focus on Privacy, Data Security, and Critical Infrastructure Protection
- GA's asked to prepare and submit Self-Assessment Forms

To help focus attention and strengthen the GA's security and privacy practices.

How We Did It...

- Used a risk-based approach
 - Portfolio Size
 - Risk Profile
 - Agency Size
 - Results from self-assessment questionnaire
- Conducted site reviews on 15 of the 32 Guaranty Agencies
- Reviews represent 86% of the total FY10 GA portfolio of \$410B

How We Did It...(cont'd.)

- Prepared and Distributed Pre-Visit Questionnaires
- Performed Market Research on each GA
 - Review 10K Reports
 - Google and Blog Searches
 - Recent Audit and SAS70 Reports
- Reviewed System Security Plans (SSP's)

What We Did...

- FSA Team (4 individuals) performed a day long visit at each site
- GA Senior Management presented the opening briefing
- Team reviewed and validated information submitted in pre-visit package
- Engaged Guaranty Agency technical team (CIO, CISO, Audit Manager, etc.)

What We Did...(cont'd.)

- Conducted in depth discussions based on risk categories/groupings
 - Logical Access Control
 - Critical Infrastructure
 - Strategy
 - Incident/Breach Response
 - Monitoring/Vulnerability Management
 - Governance

What We Did...(cont'd.)

- Reviewed Guaranty Agency's processes, policies, and procedures
- Visited Data Center
- Conducted Operational Unit tour (vault, call center, etc.)
- Presented out brief to GA Senior Management
- Prepared and distributed report highlighting observations and recommendations
- Received, reviewed, and recorded GA management responses

What We Found...

Overall observations (**SWOT** analysis)

- **Strengths**
 - Critical Infrastructure Protection
 - Governance
- **Weaknesses**
 - Strategy
 - Incident Breach Response

What We Found...(cont'd.)

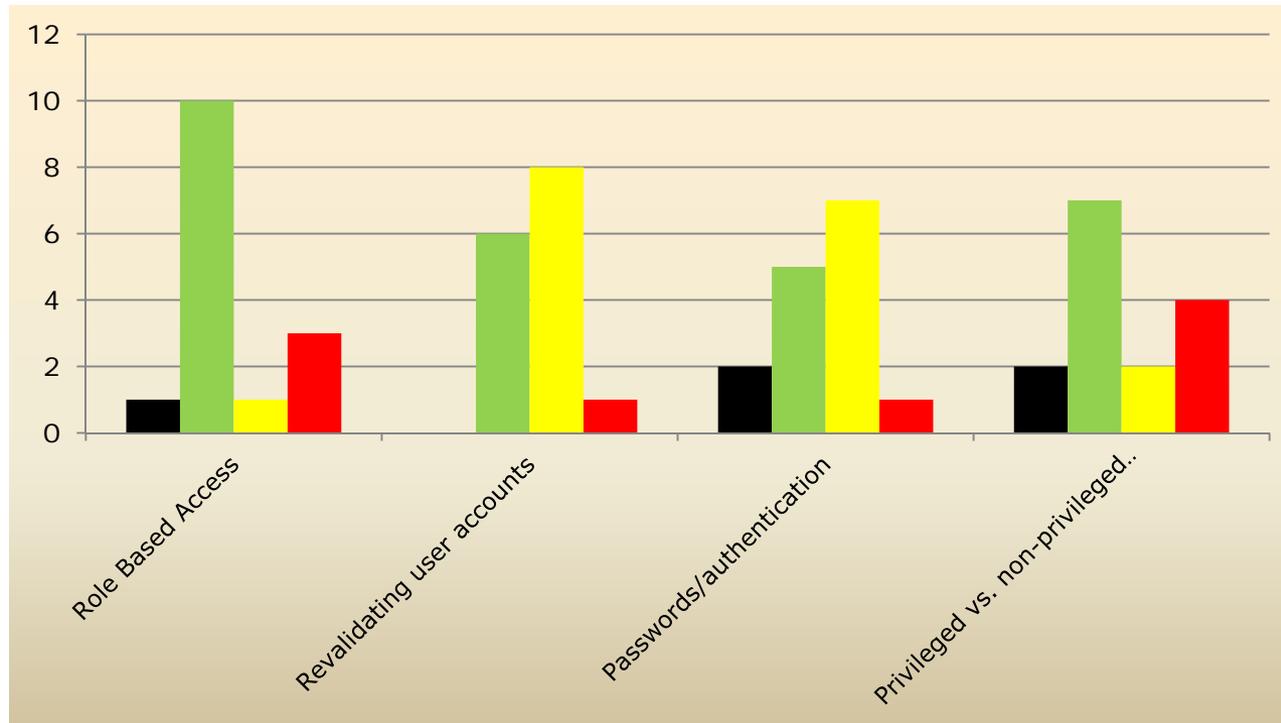
- **Opportunities**
 - Update and embellish policies/processes
 - Improve communication between GA's and service partners
 - Improve certification of technical staff
 - Create and expand on the trusted relationship between FSA and the GA's
- **Threats**
 - Weak Monitoring
 - Revalidating user accounts

Summary of Reviews

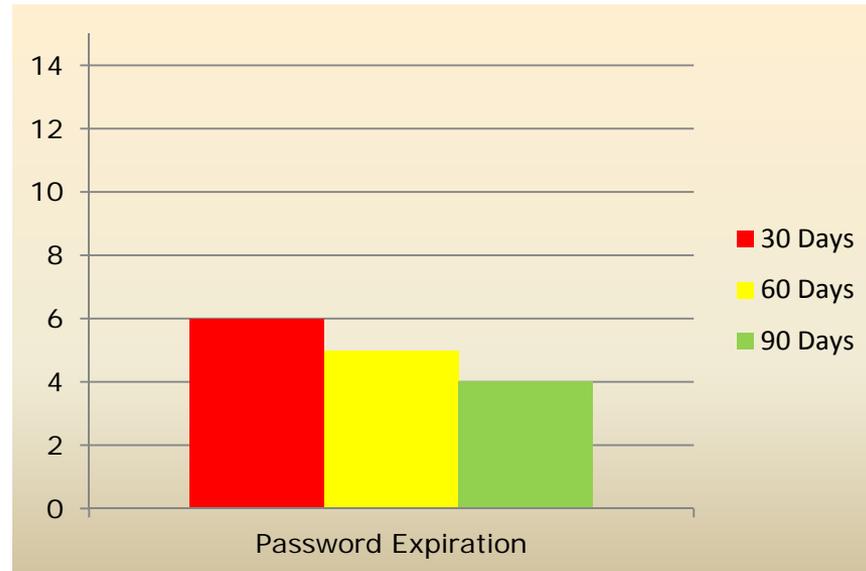
	Logical Access Control	Critical Infrastructure Protection	Strategy	Incident/Breach Response	Monitoring	Governance
1)	1	1	2	2	3	2
2)	2	1	2	2	1	1
3)	1	1	1	2	1	1
4)	1	2	1	1	2	1
5)	2	2	2	2	2	2
6)	3	1	2	3	2	3
7)	1	1	2	3	1	2
8)	1	1	2	1	1	1
9)	1	1	1	2	1	1
10)	3	1	2	2	2	2
11)	2	1	2	1	1	1
12)	3	2	3	3	3	2
13)	1	1	1	1	1	1
14)	1	1	1	1	1	1
15)	1	1	1	1	1	1



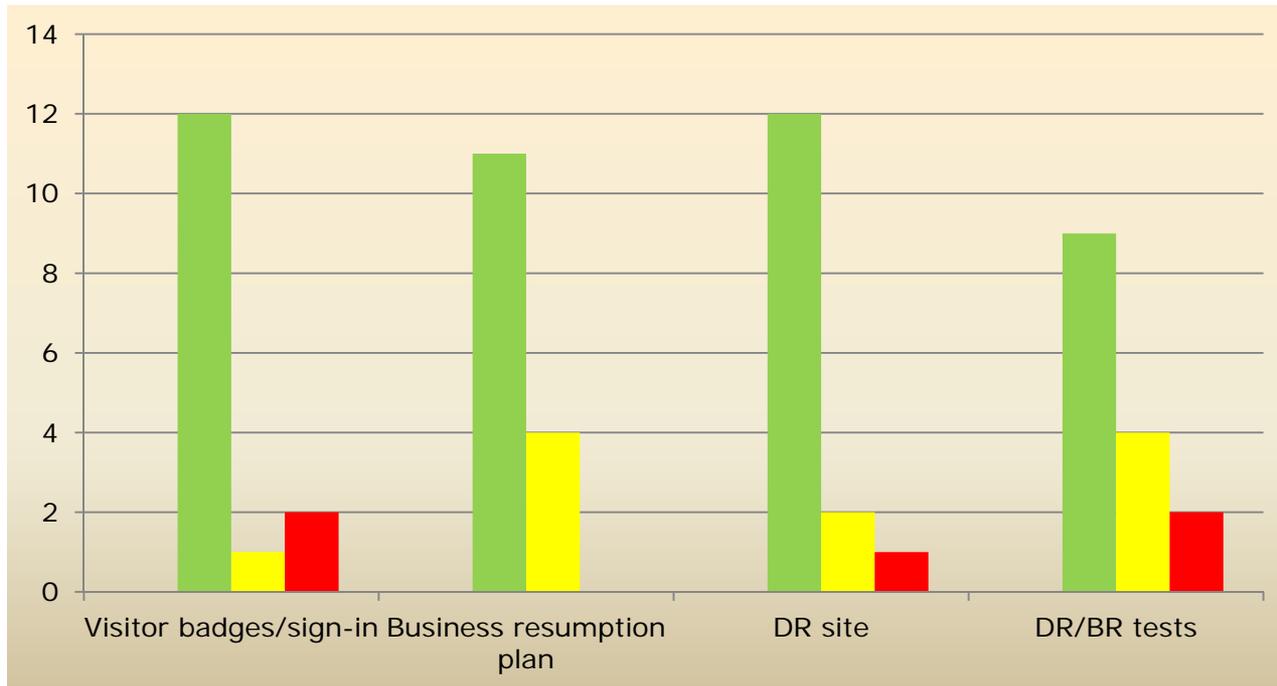
Logical Access Control



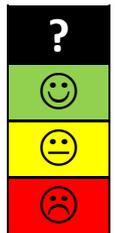
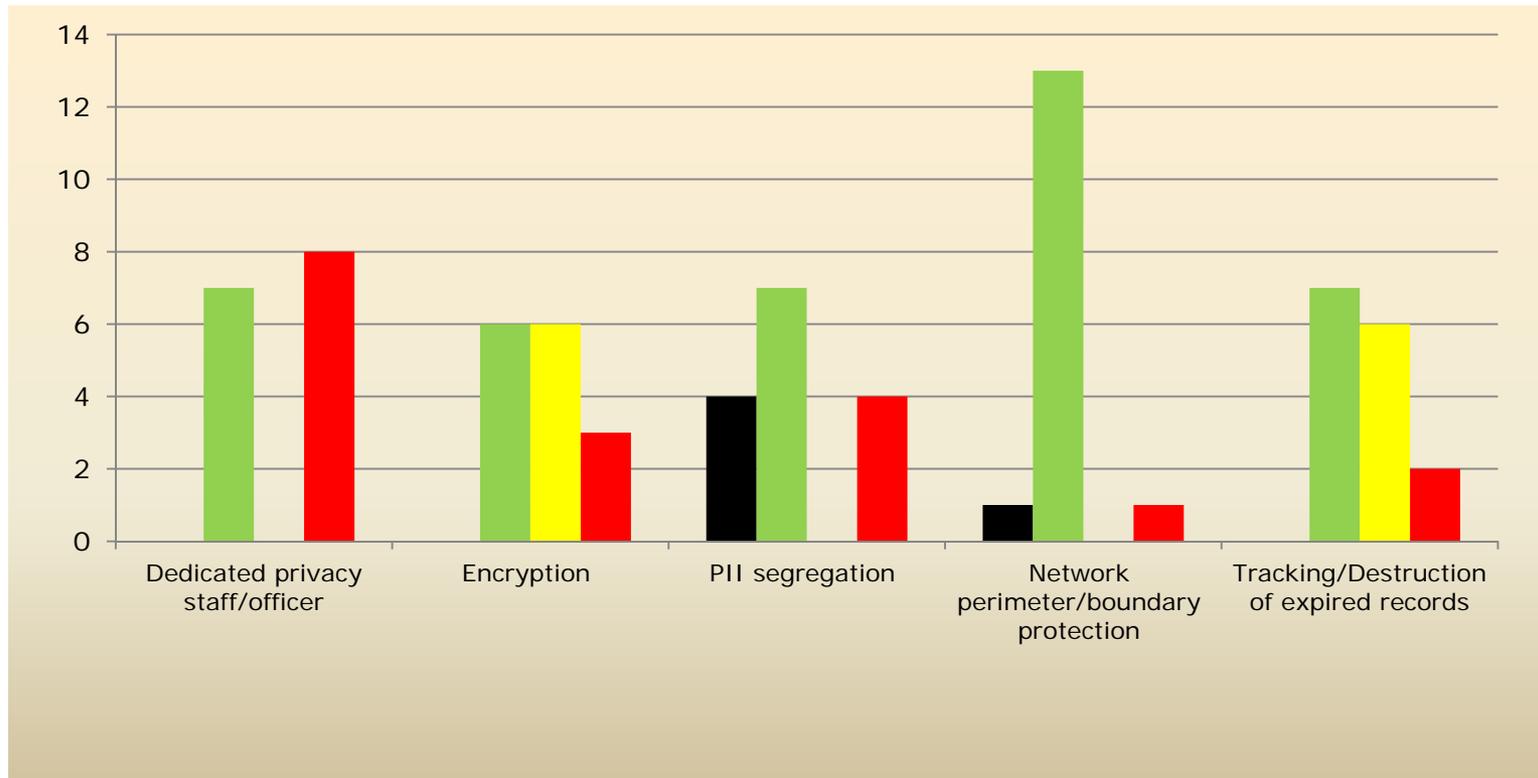
Logical Access Control



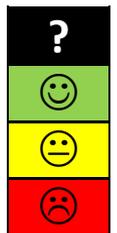
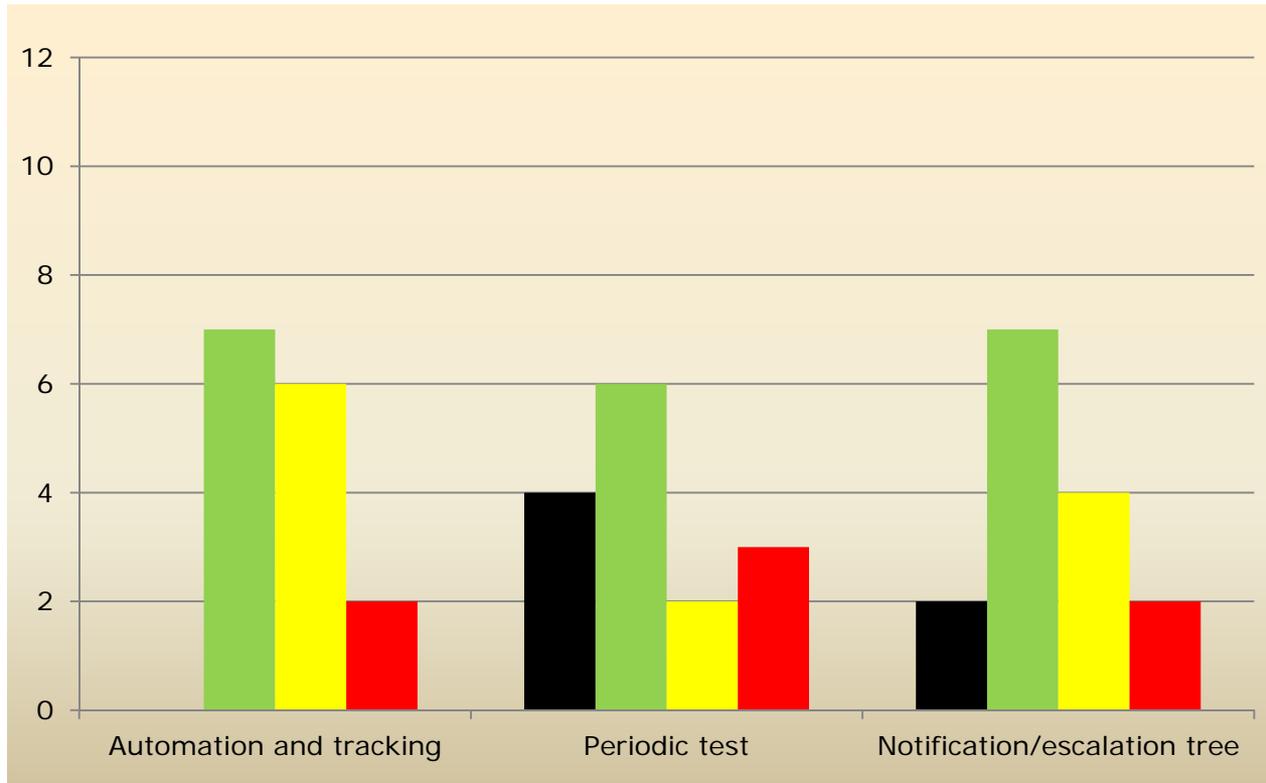
Critical Infrastructure Protection



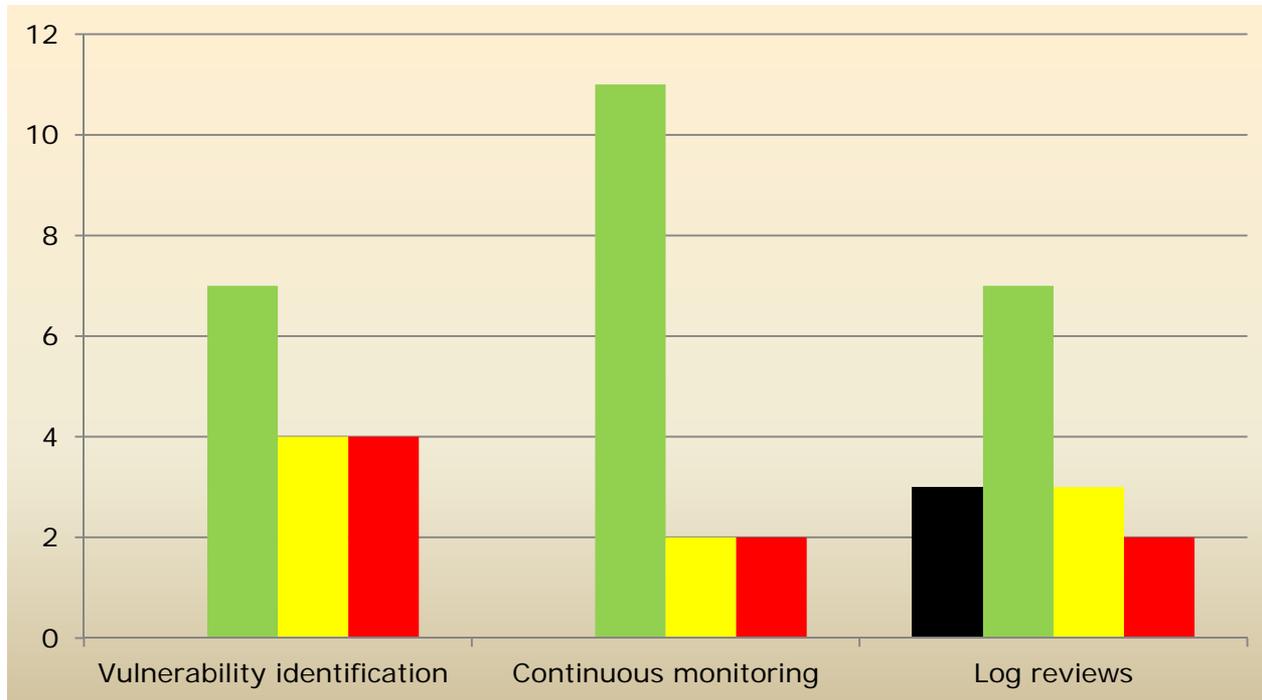
Strategy



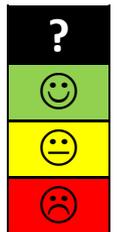
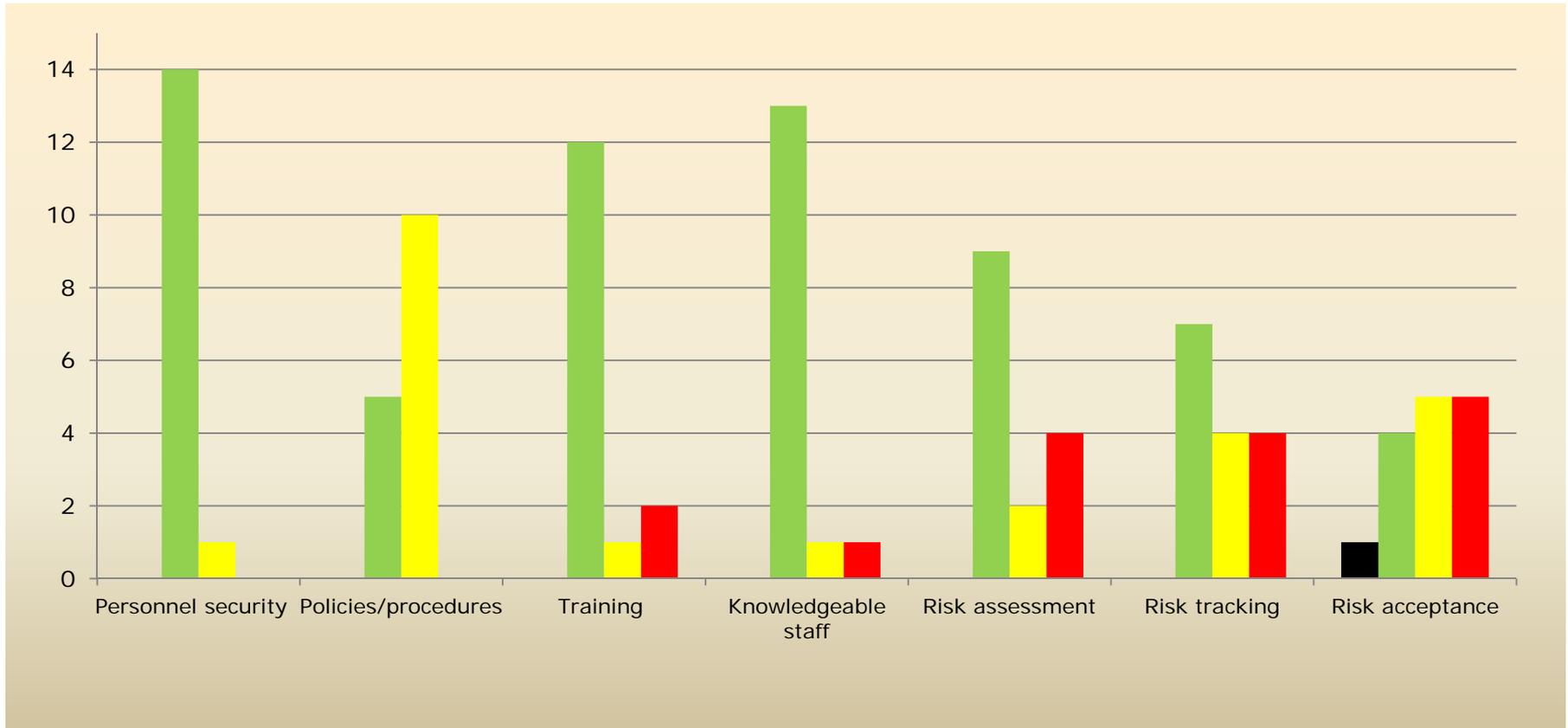
Incident/Breach Response



Monitoring (Vulnerability Management)



Governance



Next Steps...

- Monitor the individual GA Remediation Plans
- Conduct additional GA visits
- Finalize overall GA assessment reports
- Conduct repeat visits as required
- Explore ways for continued collaboration with the GA community

GOAL – To improve overall GA security posture.

Contact Information

We appreciate your feedback & comments.

Bridget-Anne Hampden
Deputy CIO

- E-mail: Bridget-Anne.Hampden@ed.gov
- Phone: 202-377-3508

Critical Infrastructure Protection (Contingency Planning)

Brian Lecher

**Pennsylvania Higher Education Assistance Agency
(PHEAA)**



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Contingency Planning Objectives

- Anticipate, react to, and recover from events that threaten the security of information assets in the organization and to subsequently restore the organization to normal modes of business operations
- Enable PHEAA to continue services to FSA, students, schools and clients
- Minimize financial losses
- Mitigate negative effects on strategic plans, operations, business reputation, market standing, and compliance with applicable laws and regulations

Planning Prerequisites

- **Identify business critical functions**
 - Business Impact Analysis - Identify potential impact of non-specific events on functions, maximum allowable downtime, and levels of acceptable losses (data, operations, financial)

- **Identify resources that support critical functions**
 - Map technical infrastructure to BIA results
 - Consider data backup strategy and data synchronization
 - Establish Recovery Point Objective - maximum amount of data loss in the event of a disaster
 - Establish Recovery Time Objective - maximum amount of time it takes to go from plan activation to fully operational, tested system

- **Anticipate potential contingencies or disasters**
 - Risk Assessment - Analyze potential business disruptions and threats based upon severity and likelihood of occurrence



Plan Preparation

- **Select and develop contingency strategies**
 - Notification/Activation-Detect and assess damage and activate the plan
 - Recovery- Restore temporary IT operations and recover damage done to the original system
 - Reconstitution- Restore IT system processing capabilities to normal operations
- **Implement changes to support the contingency strategies**
- **Test and revise the strategies**

PHEAA's Approach

- **Data center is designed to continue functioning without utility power**
 - Uninterruptible Power Supply (UPS) provides short-term protection
 - Diesel generator provides full emergency electrical power
 - Backup infrastructure tested quarterly
- **Network architecture based on load sharing, multiple paths and redundancy**
 - Production network connections between operations centers, data center and disaster recovery site
- **All data/systems backed up daily**
 - Physical and/or virtual data stored offsite
 - Data retained according to defined schedule
- **Comprehensive disaster recovery and business continuity plan (Enterprise Business Continuity Plan)**

Enterprise Business Continuity Plan

- Formalized, structured approach involves all levels of staff, including executive management and CEO
- Addresses roles, responsibilities, tasks, assignments, and contact information
- Liaisons for each business unit assigned to review, update, and disseminate plans
- Plans updated and approved at VP level at least quarterly
- Individuals assigned to teams covering enterprise tasks, such as logistics, human resources, facility recovery, etc.



Testing Approach

- **Contingency plans tested annually to validate that we can successfully restore all critical systems in expected timeframes**
- **Plan utilizes off-site, geographically diverse vendor support for restoration of systems/data and business continuity services**
 - Primary recovery site provides comparable equipment to support IT data/system recovery as well as 'hot site' seats for continuity of business operations
 - Other vendors provide continuity services for print/mail and payment processing operations
 - Externally-hosted emergency notification system provides mass distribution capability for email/phone messages and updates
- **Success of comprehensive test relies on coordination among all support components**



Testing Results

- **2011 Exercise**
 - All critical systems recovered and verified
 - 1,800 tasks
 - 195 participants
 - 4 physical locations
- **All activities are fully documented and audited**
- **Post-test participant survey and lessons learned session**
- **Response capability tested and refined via real world incidents (utility outages, flooding)**



Considerations

- **Selecting your testing window**
- **Ensuring that critical software and hardware system specifications are covered in vendor contracts**
- **Deciding on degradation plans, if any**
- **Planning for post-incident moves -'hot' to 'cold' site and beyond**

Contact Information

We appreciate your feedback & comments.

Brian Lecher, CIO

- E-mail: blecher@pheaa.org
- Phone: 717-720-3262

Protecting Data at the Endpoints

David Lentz
Great Lakes Higher Education
Corporation



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Do you know your Endpoints?

- PCs
- Laptops, notebooks computers, etc.
- Tablets
- Smartphones and other e-mail capable devices
- Printers, copiers, fax machines if connected to your network
- Web portals, e-mail servers
- Wireless access devices

Do your endpoint devices retain a copy of files or images?

- Word processing programs commonly save draft copies of documents at timed intervals on local drives. Those copies stay on the machine until they are explicitly deleted

Do you have clear guidelines on how to decommission and dispose of endpoint devices?

- Do you want to buy back recycled disk drives or USB devices that have your data on them?

Can users load data or executable code to or from endpoint devices using removable media or devices?

- Do you have adequate information about and control of what they put on or take off of your endpoint devices?

Are your endpoint devices shared?

- You need to enforce identification and authorization of the device users, and to prevent the exposure of information authorized for one user to any subsequent users

Are your endpoint devices appropriately protected?

- Malware protection
- Firewall settings
- Disk encryption
- How do you handle devices that are only occasionally connected to your network?

How frequently do you need to assess the security of your endpoint devices?

Are your endpoint device users trained to be good guardians of their data?

- Do they know how to report inappropriate exposure of sensitive data?

Reference Material

- The National Institute of Standards and Technology, in their Special Publications 800 series (NIST SP 800)

Contact Information

We appreciate your feedback & comments.

David Lentz, CTO

- E-mail: dlentz@glhec.org
- Phone: 608-246-1409

Incident Response – Plan for failure

Vincent Grimard
Nelnet



It's not "if" it's "when"

- As a leader, accept your fate, with chaos comes opportunity, fear is an illusion
- The key element in continuing to protect PII and your organization will be your ability to plan for and respond to an incident
- A successful implementation depends on a plan that matches well with your organization, teams and clients
- Guideline: NIST 800-61

6 Steps To Incident Success

- **Preparation**
- Identification
- Containment
- Eradication
- Recovery
- **Lessons Learned**

If you fail to plan, plan to fail

- Not all events are created equal
- Build your core team
- Identify your extended team
- Define roles and responsibilities
- Build strategic/asset based relationships
- Define your incident command structure
- Be proactive
 - Build an Enterprise Council
 - Find Likeminded People

Know and Understand

- **Assess the situation**
 - Ask the right questions
- **State Laws**
 - When to contact
 - How to contact
- **Contractual Requirements**
 - Know your SLA's and responsibilities
- **FSA partners**
 - Who are your internal Contact Points

Evidence and Forensics

- What does this situation require?
- Evidence should be controlled
- Mark off the area
- Post signs to inform users what not to touch and who to contact
- Contain evidence in tamper proof bags
- Document all access to the safe or cabinet where evidence is kept
- Mark all evidence with a date and time

10 Most Common Mistakes

- Inaccurately evaluating the situation
- Missing or Untested Backups
- Inadequate or Non-Existent Documentation
- Evidence Handling Failures
- Communication Breakdowns
- Failure to ask for help
- Failure To Plan
- Failure to Test
- Stress Management
- Lack of Lessons Learned

Contact Information

We appreciate your feedback & comments.

Vincent Grimard, Director of Security

- E-mail: vincent.grimard@nelnet.net
- Phone: 303-696-5486
- Connect with me on Linked In

Monitoring/Vulnerability Management

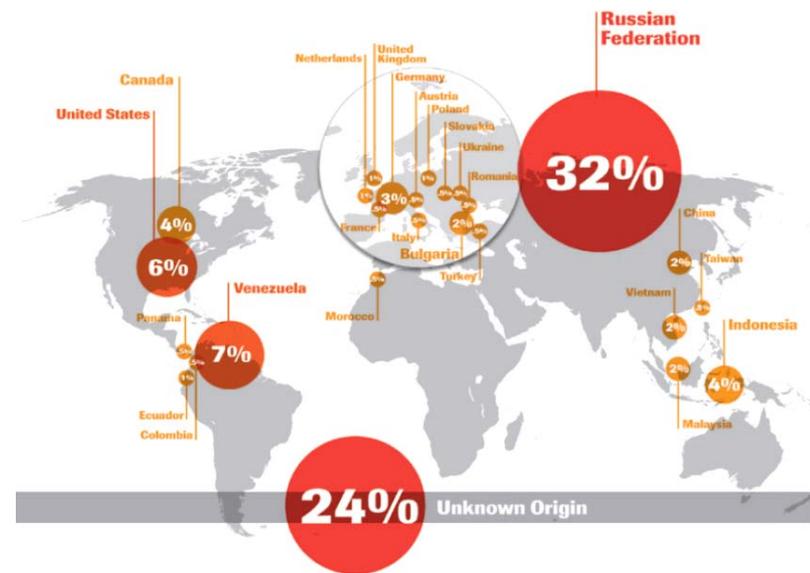
Jerry Archer
Sallie Mae



START HERE
GO FURTHER
FEDERAL STUDENT AID®

Rapidly Evolving Threats

- Advanced Persistent Threats (APTs) are reality (actually Average Persistent Threats)
- Blended Threats – cross-channel, cross-domain, cross-functional
- Cyber-criminals have significant technical means funded by criminal profits and development of nation-state capability
 - Continued rise in Day-0 and targeted attacks
- Patchwork defense characterizes current security
- Current defenses significantly undermined by rapid growth in technology
 - Cloud computing
 - Rich Internet Applications (RIAs)
 - Mash-ups
- Third party risk and transparency are growing concerns
- Compliance burden is dramatically increasing and is, generally, not accretive to improving the security posture



Defense-in-Depth Necessary But Not Sufficient

- Highly agile adversaries quickly exploit vulnerabilities
- Day-0 vulnerabilities abound and immune to signature-based defense
- Force multipliers on the order of 10,000 to 1
 - Boundary defense becomes very expensive and impractical against well-funded cyber-criminals and nation-states
- APTs complicated to detect or block
 - Blended attacks are designed to be stealthy
 - Patchwork of non-integrated defenses make it difficult to detect subtleties of attacks

Cybercriminals are repeatedly portrayed as individuals or a loosely connected band of individuals. But our research demonstrates that cybercriminals have evolved to integrate with the world's organized crime rings. These criminal organizations are highly structured and are now investing in technology and technically skilled people to assist them in a primary goal: defrauding businesses worldwide.



START HERE
GO FURTHER
FEDERAL STUDENT AID

Changing Trajectory

When you get to a fork in the road take it.

-- *Yogi Berra*



START HERE
GO FURTHER
FEDERAL STUDENT AID

Resilient Defense - Strategically

- Identify and minimize likely targets and threats
 - Attack agility is significantly diminished when the objective is fixed or limited
- Interplay between inbound penetration and outbound exfiltration create increased visibility and thus detection opportunities
- Limiting criminal objectives means:
 - Defense becomes much more tractable
 - Well defined and can be rationalized/prioritized
 - Defense resources focused on threats which are economically feasible
- Integrating defense and intelligence create game-changer

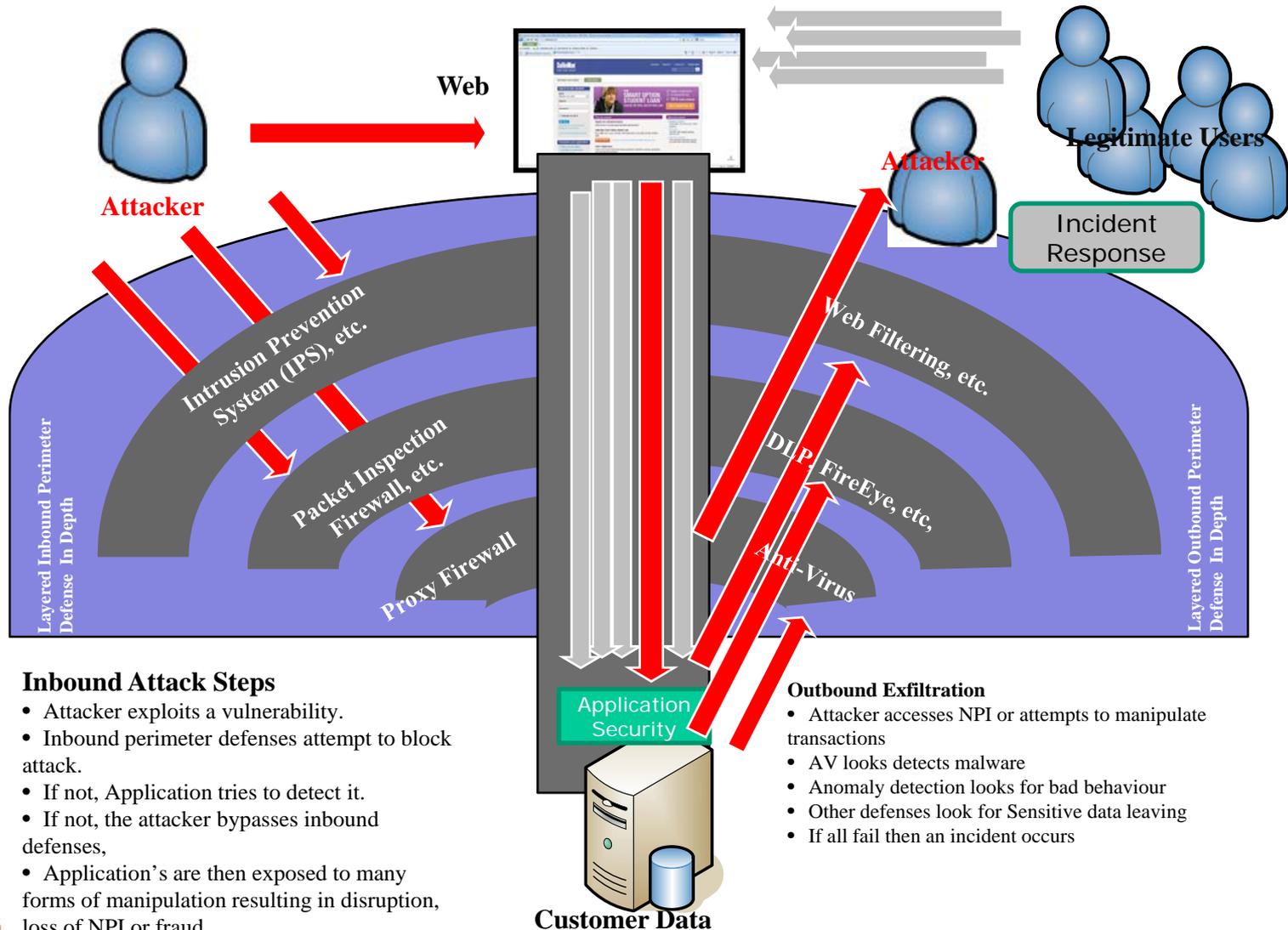


Priorities: Detect, Deflect, Deter, Defend



START HERE
GO FURTHER
FEDERAL STUDENT AID

Resilient Defense



Inbound Attack Steps

- Attacker exploits a vulnerability.
- Inbound perimeter defenses attempt to block attack.
- If not, Application tries to detect it.
- If not, the attacker bypasses inbound defenses,
- Application's are then exposed to many forms of manipulation resulting in disruption, loss of NPI or fraud.

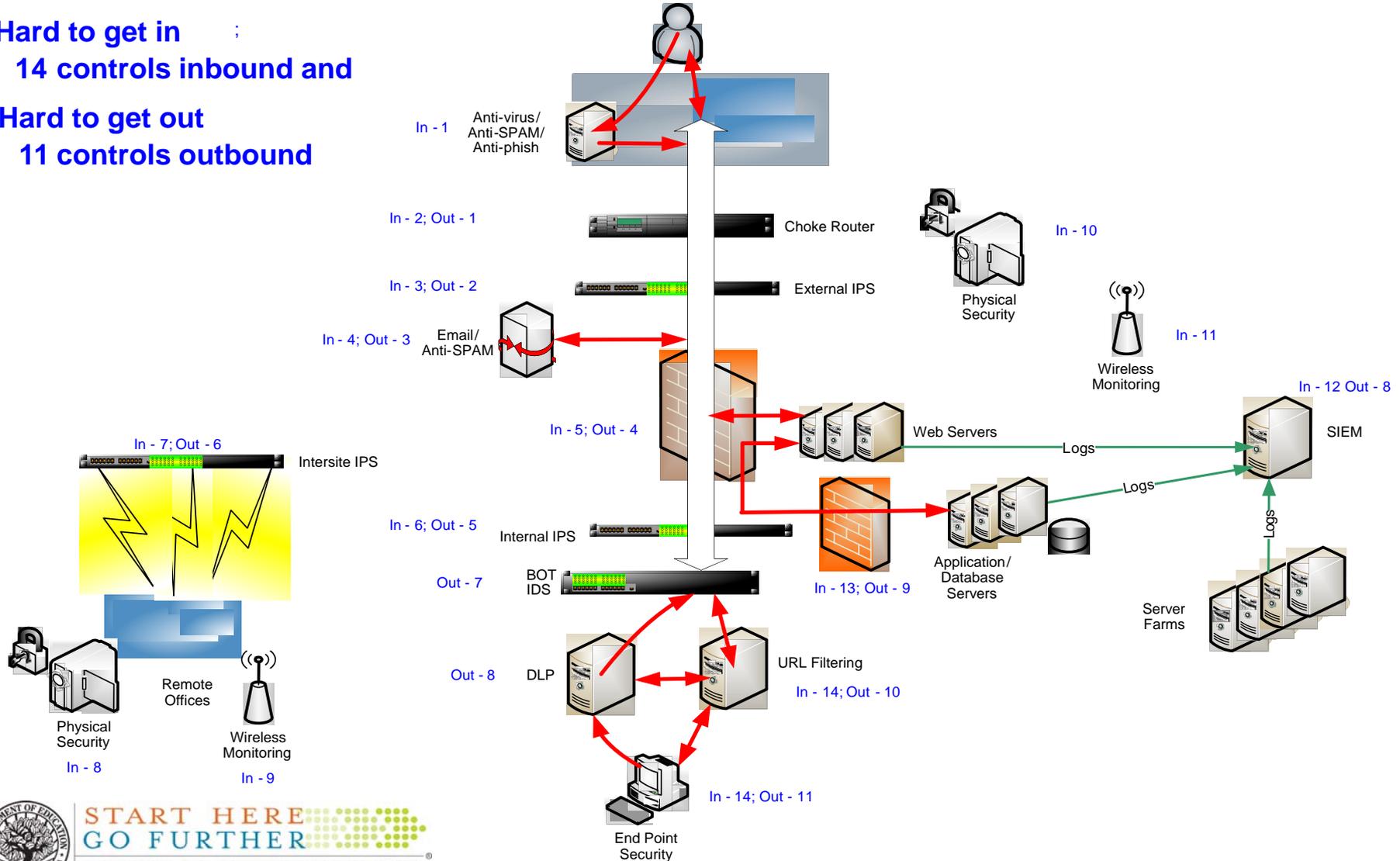
Outbound Exfiltration

- Attacker accesses NPI or attempts to manipulate transactions
- AV looks detects malware
- Anomaly detection looks for bad behaviour
- Other defenses look for Sensitive data leaving
- If all fail then an incident occurs



Sallie Mae Resilient Defense

Hard to get in :
 14 controls inbound and
 Hard to get out
 11 controls outbound



Contact Information

We appreciate your feedback & comments.

Jerry Archer, SVP, CSO

- E-mail: jerry.archer@salliemae.com
- Phone: 703-984-5807