

Data Security Initiatives

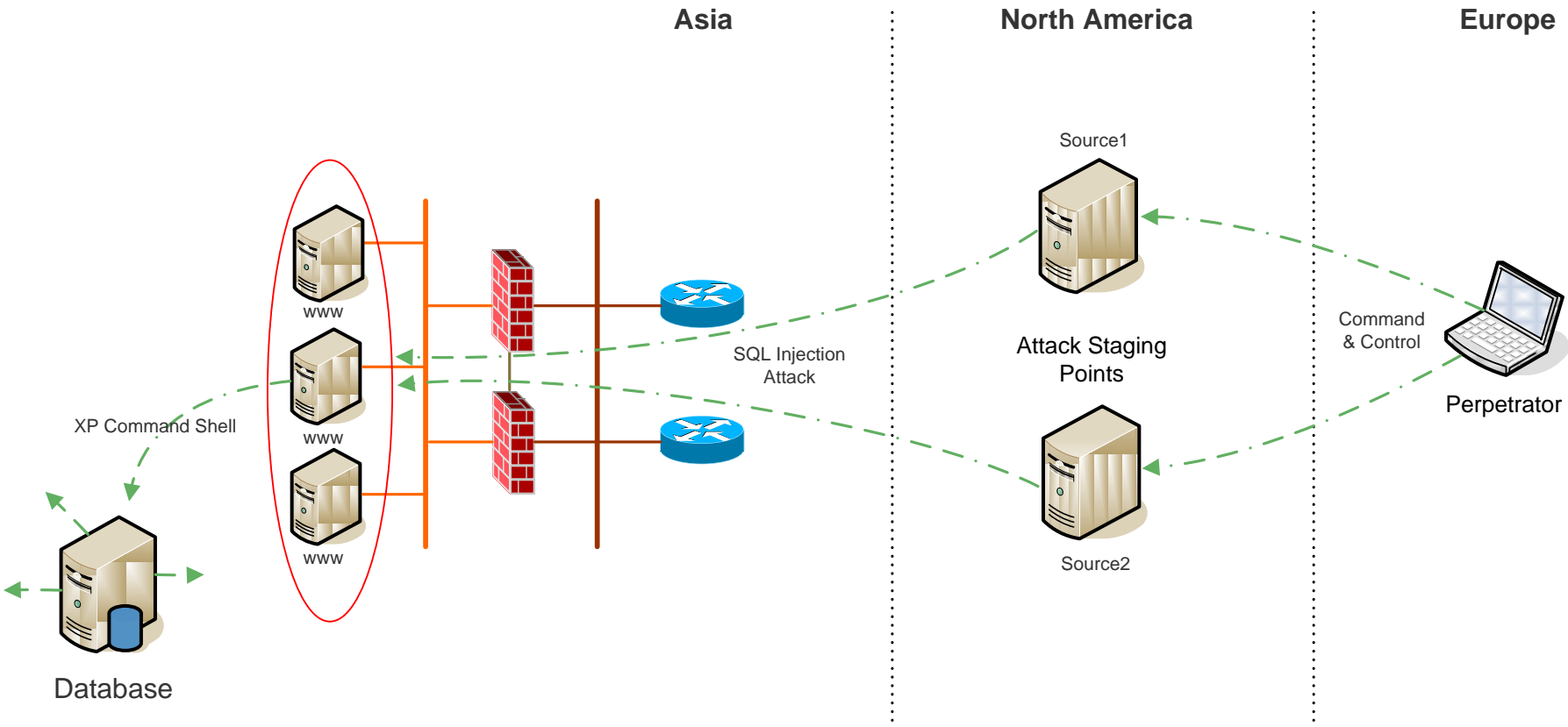
The Layered Approach

Melissa Perisce

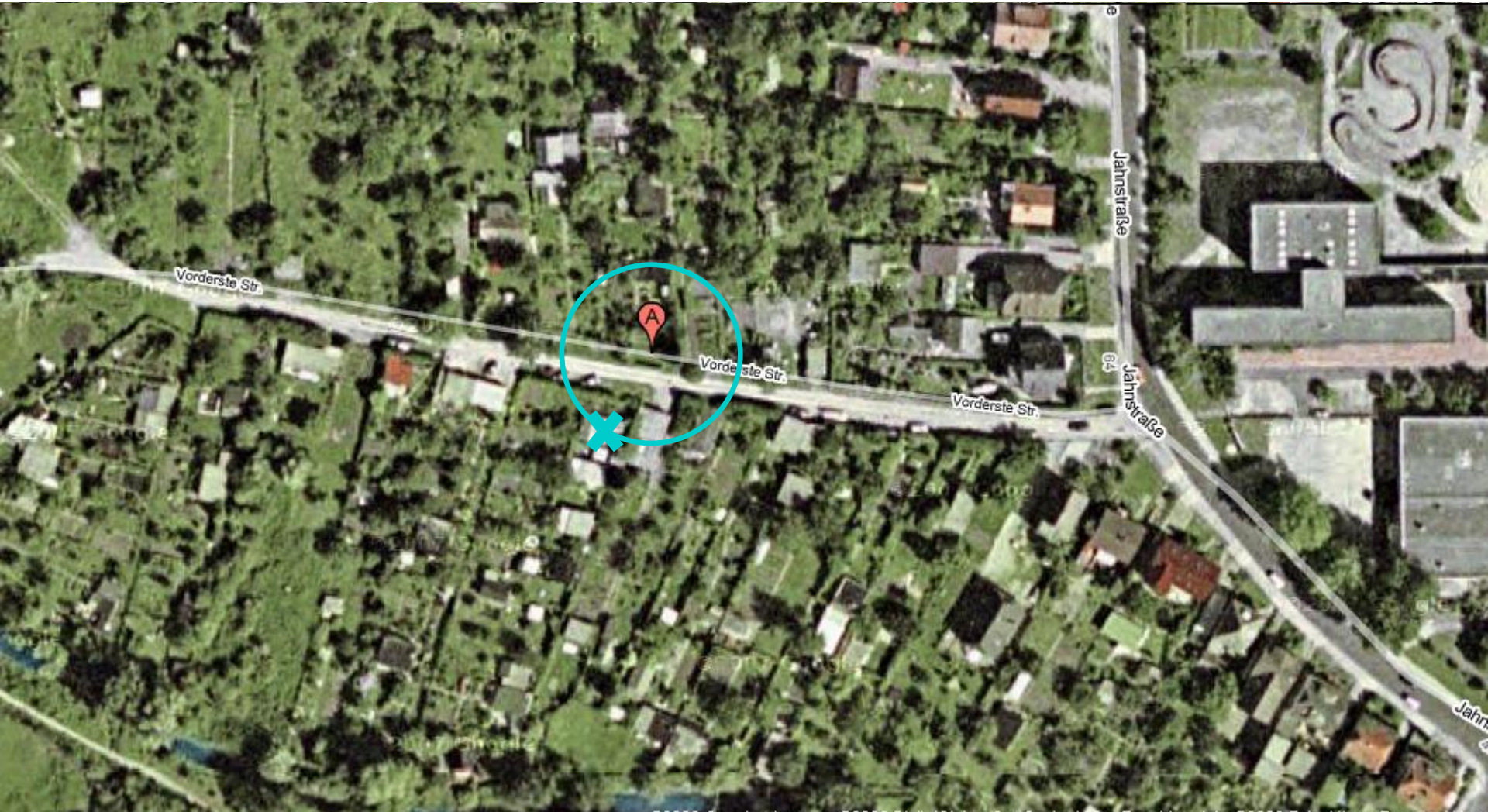
Regional Director, Global Services, South Asia

April 25, 2010

Intel Case Study



Case Study (continued)



Breach Sources

External sources

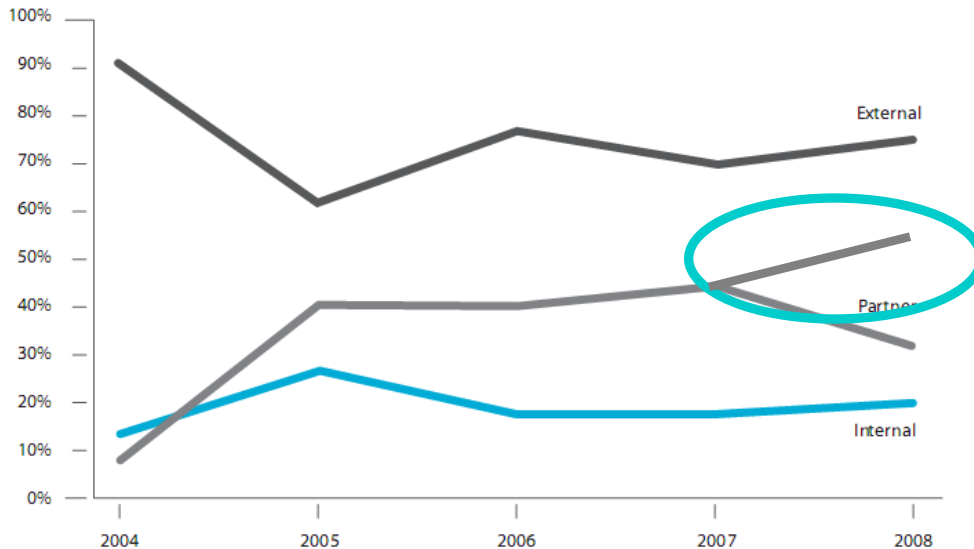
- Most breaches, nearly all records
- 90+% of breached records attributed to organised crime activity

Internal sources

- Roughly equal between end-users and admins

Partner sources

- Mostly hijacked third-party accounts/connections



Likelihood

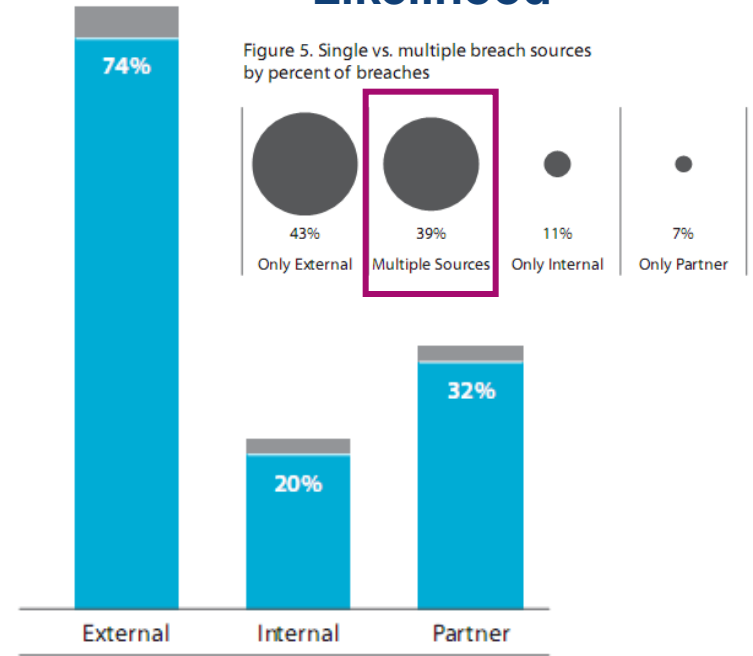
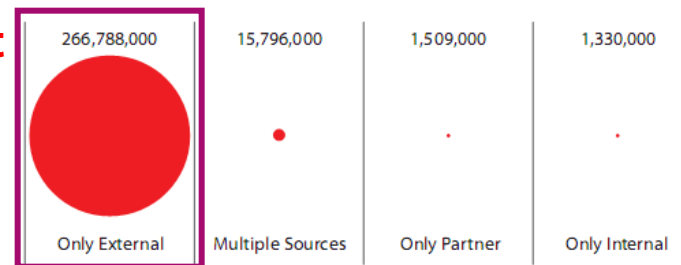


Figure 8. Total records compromised by source

Impact



Compromised Assets and Data

Most data breached from online systems

- Different than public disclosures

Criminals seek payment card data

- Easily convertible to cash

Other types common as well

- Auth credentials allow deeper access
- Intellectual property at 5-year high

Figure 25. Asset classes by percent of breaches (black) and records (red)

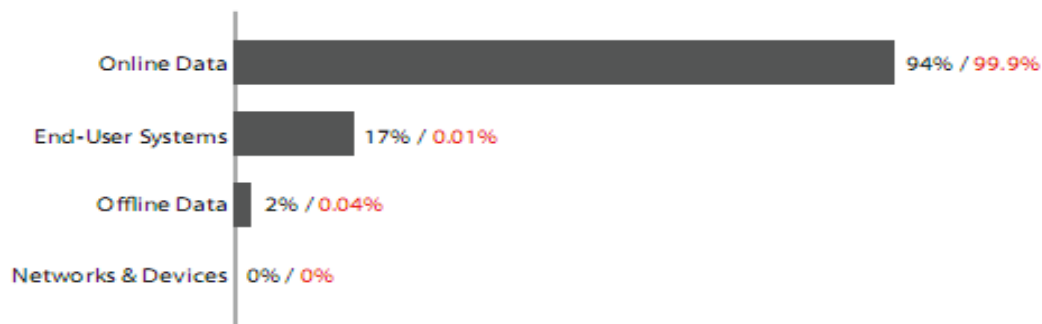
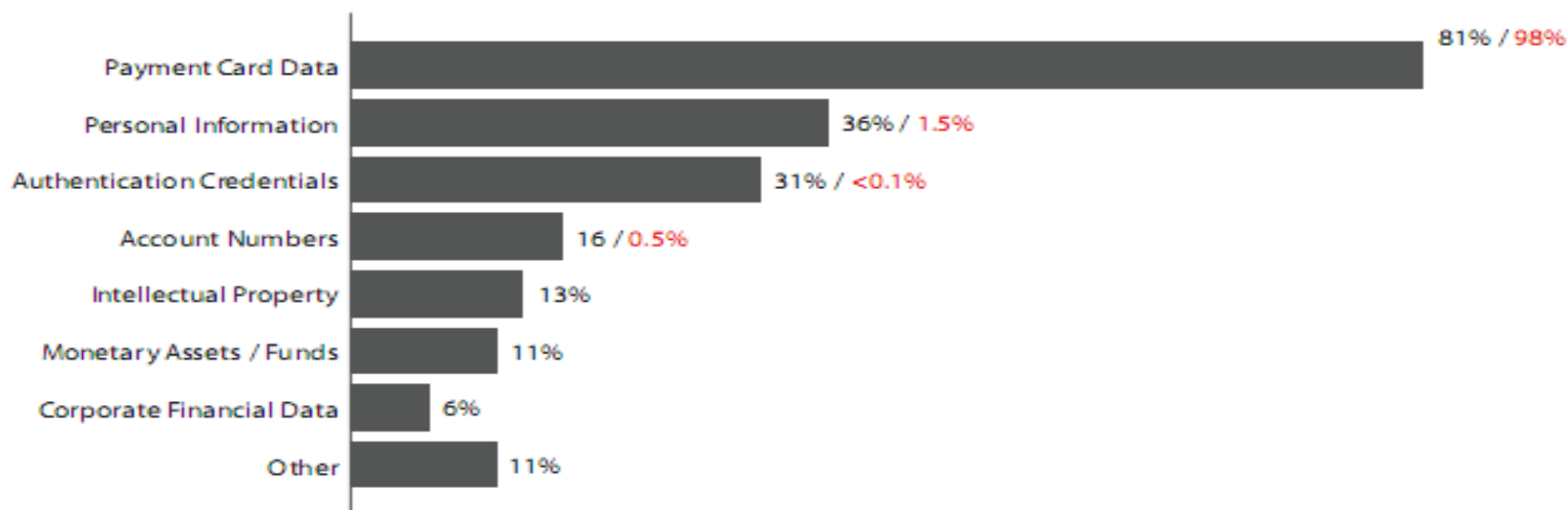


Figure 29. Compromised data types by percent of breaches (black) and records (red)*



The Extended Enterprise Comes With New Security Challenges

Measuring against risk

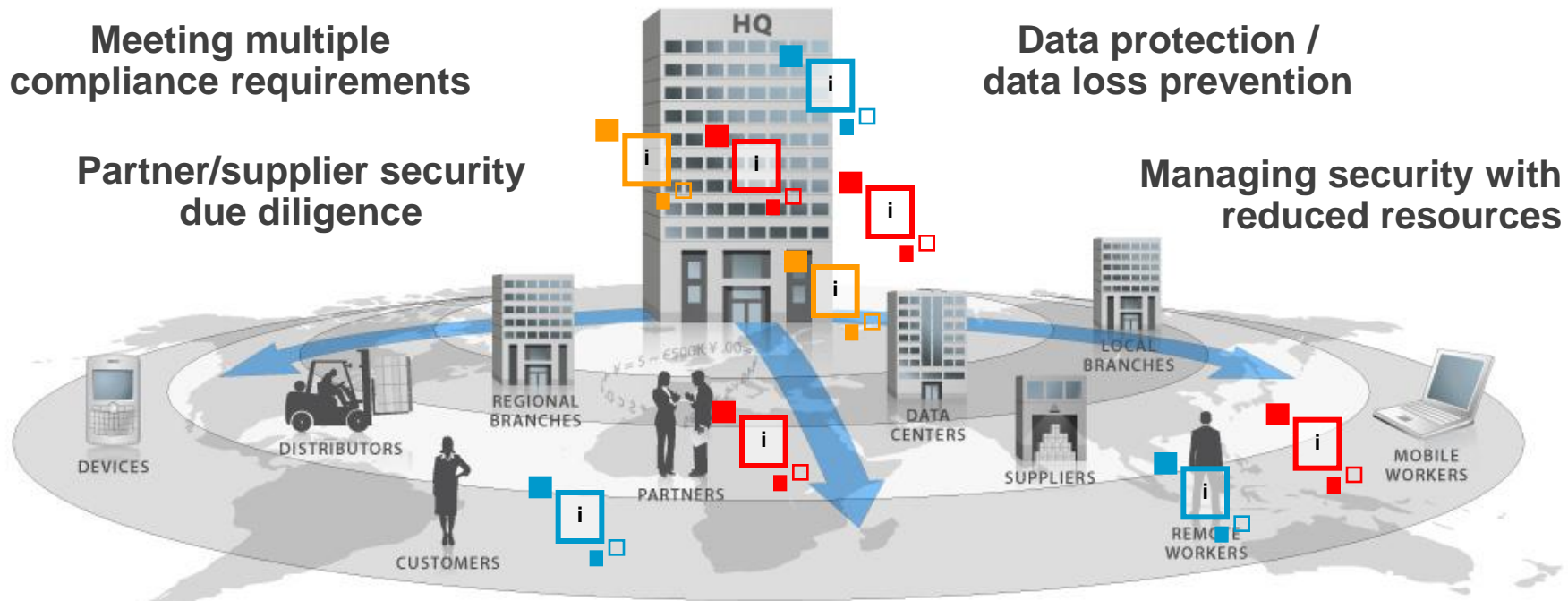
Application security

Meeting multiple compliance requirements

Data protection / data loss prevention

Partner/supplier security due diligence

Managing security with reduced resources



Ongoing monitoring and management

Business continuity

Security log data handling

Consumer/employee mobility

The Evolving Security Market Changes Require a New Approach

Wider

Security controls should span the Extended Enterprise and should be executed where they are most effective and cost-efficient



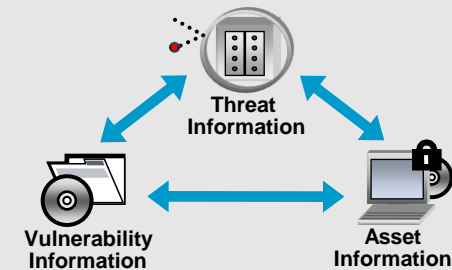
Deeper

Security should span the entire IT stack, including the network, data, applications, and users



Smarter

Security decisions should be based on risk, not on just threats and vulnerabilities



Securing the Enterprise : The Layers

Challenges	Issue	Solutions
<ul style="list-style-type: none">• Measuring against risk• Addressing multiple compliance requirements• Third party security due diligence	Governance, Risk and Compliance	<ul style="list-style-type: none">• Risk management services• Security compliance services• PCI DSS assessment and audit (QSA)
<ul style="list-style-type: none">• Application security• Data protection/ data loss prevention• Information access control	Securing the Information	<ul style="list-style-type: none">• Data classification and data discovery• Application security• Identity and access management• Forensics and incident response
<ul style="list-style-type: none">• Ongoing monitoring and management• Security log data handling• Business continuity• Consumer/employee mobility	Securing the Infrastructure	<ul style="list-style-type: none">• Security policy definition and review• Security architecture design and review• Security technology implementation• Security Operations Services• Vulnerability assessment and penetration testing• Business continuity and disaster recovery

Risk and Compliance: Key questions

Risk, and
Compliance

Securing the
Information

Securing the
Infrastructure

- **Measuring against risk**
 - Are you able to measure which security controls result in most risk reduction?
 - Do you know whether your overall risk is increasing or decreasing?
 - How does your risk profile compare to that of your peers?
- **Addressing multiple compliance requirements**
 - Are you able to keep up with the growing amount of security compliance requirements?
 - Have you established a cost-efficient program that allows measuring once while reporting against multiple standards and regulations?
- **Third party security due diligence**
 - Do you assess third party security risk?
 - Do you know how to measure, track and manage third party risk?

Securing the Information: Key questions

Risk, and
Compliance

Securing the
Information

Securing the
Infrastructure

- **Application security**

- Do you know whether or not your business applications are vulnerable to attacks?
- Do you have security controls in place that protect your web-based business applications?

- **Data protection / data loss prevention**

- Do you know where critical data resides in your organization?
- Are you able to detect data loss should it occur?
- Are you prepared to respond to a security breach?

- **Information access control**

- Do you know who accesses information?
- Are you able to detect unauthorized information access?

Securing the Infrastructure: Key questions

Risk, and
Compliance

Securing the
Information

Securing the
Infrastructure

- **Ongoing monitoring and management**
 - Do you monitor security logs and alerts on a 24 by 7 basis to discover security incidents swiftly?
 - Do you keep your security infrastructure up to date with the changing threat landscape?
 - Do you know how to prioritize remediating vulnerabilities?
- **Security log handling**
 - Do you know how to store and query security raw data in view of compliance requirements and audits?
- **Business continuity**
 - Are you prepared to securely recover after a disaster?
- **Endpoint security**
 - Do you know how to secure mobile endpoints (laptops)?

What Is PCI DSS?

Main Purpose:

- Protect Cardholder Data
- Reduce Fraud

Target:

- “...requirements apply to all members, merchants, and service providers that store, process, or transmit cardholder data.”

More Info:



www.pcissc.org

- The Payment Card Industry (PCI) Data Security Standard
- Jointly developed by VISA and MasterCard
- The PCI program is designed to protect cardholder data.
- Compliance is required of all merchants and service providers that store, process, or transmit cardholder data.
- Adopters of the standard include American Express, Diners Club, Discover, and JCB International



Top Security Projects for 2010

Figure 1. 2010 Security Technology Project Priorities

Security Project Portfolio Placement (Listed in "Top 5" Priorities)

Top Security Project Priority (Listed as No. 1 Project)

Ranking			Ranking		
1	Intrusion Prevention	47.5%	1	Identity Management	20.5%
2	Patch Management	46.1%	2	Data Loss Prevention	13.9%
3	Data Loss Prevention	44.5%	3	Antivirus	10.6%
4	Antivirus	41.1%	4	Firewalls	9.3%
4	Identity Management	41.1%	5	Intrusion Prevention	8.6%
6	Firewalls	37.4%	6	Network Access Control	7.3%
6	Vulnerability Assessment	37.4%	6	Patch Management	7.3%
8	Network Access Control	35.5%	8	Security Information and Event Management	5.3%
8	Security Information and Event Management	35.5%	9	Strong User Authentication	4.6%
10	Remote-Access or Site-to-Site VPN	31.2%	10	Remote-Access or Site-to-Site VPN	4.0%

N= 308

Source: Gartner IT Key Metrics Data 2010 (December 2009)

PCI DSS

Post-breach mapping

Table 10. Results of post-breach PCI DSS reviews conducted by Verizon Business IR. Values represent the percentage of organizations for which each requirement was found to be in place.

Build and Maintain a Secure Network	Compliance
Requirement 1: Install and maintain a firewall configuration to protect data.	30%
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.	49%
Protect Cardholder Data	
Requirement 3: Protect stored data.	11%
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.	68%
Maintain a Vulnerability Management Program	
Requirement 5: Use and regularly update AV.	62%
Requirement 6: Develop and maintain secure systems and applications.	5%
Implement Strong Access Control Measures	
Requirement 7: Restrict access to data by business need-to-know.	24%
Requirement 8: Assign a unique ID to each person with computer access.	19%
Requirement 9: Restrict physical access to cardholder data.	43%
Regularly Monitor and Test Networks	
Requirement 10: Track and monitor all access to network resources and cardholder data.	5%
Requirement 11: Regularly test security systems and processes.	14%
Maintain an Information Security Policy	
Requirement 12: Maintain a policy that addresses information security.	14%

Verizon Business Helps Contain Attack on a Leading Financial Services Company



CUSTOMER CHALLENGES

- Despite protections in place, hackers were discovered swapping IDs, passwords, and directory listings of the financial services company; 37 systems affected
- Data criminals exploited older, legacy applications – weak links
- Logs showed the initial breach occurred 3 months before, making timing critical

VERIZON BUSINESS SOLUTION

- Verizon Business Investigative Response team traced the breach by comparing publicly facing IP addresses with a dynamic “watch list”
- U.S. Secret Service joined, sharing details of a suspected organized crime syndicate with a similar M.O.

BUSINESS RESULTS

- The team’s efforts helped lead to the arrest and conviction of three individuals
- No critical data was compromised
- Implementing multiple layers of security, coupled with access to multi-tiered investigative resources, helped rapidly contain an attack

Preparing for First Contact

1. Where is the data? Identify the targets

Business segment / department

List likely compromised systems

Correlate information against major events

2. Prioritize likely compromise scenarios

Internal employee / Inside job

Vendor / other 3rd party / partial insider

Correlate information against major events

Anonymous external systems intrusion

3. Provide initial conclusions to QFI

Fraud trend/CPP is critical in determining:

- Where to look / not to look
- Approximate breach timeframe

Prove or dis-prove something specific

Save time, money, & effort investigating

External Touch-Points:

Internet connection

Wireless connectivity

3rd party connections

Remote access / VPN

Onsite Requirement

Volatile Evidence

Digital elements comprising crime scene
Subject to change / corruption / damage

Non-Volatile Evidence

Static elements from crime scene
Copies of volatile articles for analysis

Why on-site work is a must:

1. Verification & Validation

Third-party due-diligence is a must
Investigator determines what is/is not evidence
Converts volatile articles to non-volatile
Investigator must ensure chain-of-evidence

2. Accuracy & Thoroughness

Conclusions depend on evidence authenticity
Volatile evidence must be collected in-person
Volatile evidence articles cannot be shipped



High Level Investigation Phases

1. Evidence Acquisition

Duration: 1 – 4 days

On-site & target premises

Collection of digital evidence

2. Forensic Analysis

Duration: 3 – 7 days

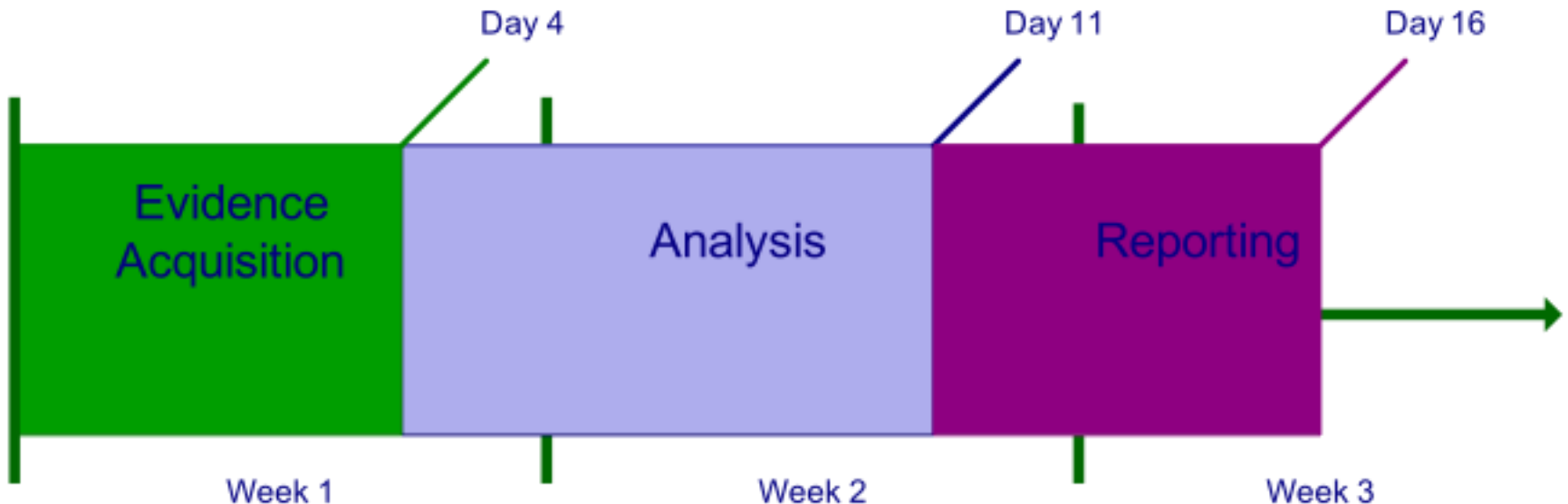
Meat of engagement

Lab environment analysis

3. Reporting

Duration: 1 – 4 days

Document facts & findings



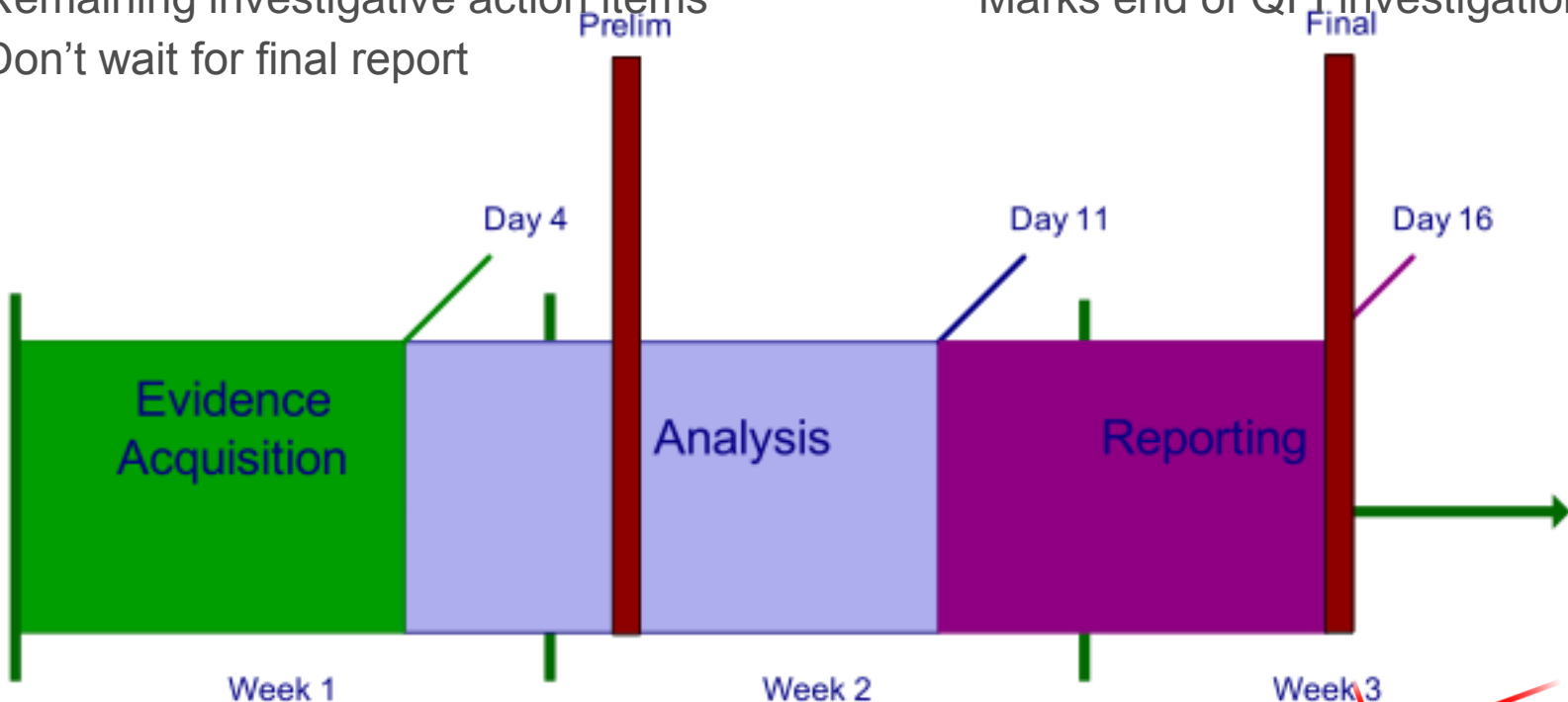
High Level Investigation Phases

1. Preliminary Findings Statement

No later than 4 days after on-site
Initial findings & conclusions
Remaining investigative action items
Don't wait for final report

2. Final Management Report

No later than 10 days after on-site
Detailed findings & case facts
Marks end of QFI investigation



Investigators Basic Measures

1. Vulnerability scanning

Target internal/external in-scope elements
External scanning before on-site starts
Identify backdoors/exposures recently seen

2. Identifying in-scope elements

Leverage fraud pattern analysis
Establish information flow diagram
Find unknown data storage points

3. System image acquisition

Personally image all in-scope systems
Perform electronic data recovery
Overlapping virus scans – 2 perspectives
Research known issues in makes/models
Master copy – Create a backup!

4. Incident response

Containment is primary focus
Recommend immediate measures
Document in Preliminary Statement

5. Forensic analysis

Expect AF techniques used
Quantify at-risk sensitive information
Calculate gross potential exposure
Use forensics to better define at-risk
Promptly furnish at-risk accounts

6. Documentation

Layout source / full extent of the breach
State whether situation is in fact contained
Follow forensics documentation guidelines

Setup A Program

1. Setup a Team

2. Discovery Meeting

- establish a baseline for processes and resources
- understand what process is in place currently for a breach
- if no process, get expert help to establish an appropriate one.
- they will also understand what resources are available and provide guidance on what is needed.

2. First Responder Training

- Develop and rollout training

Conclusions and Recommendations

You cannot prevent or detect everything.

You cannot detect everything.

Layer controls for superior effect and efficiency:

- Deter cybercrime through policies and penalties
- Keep criminals from entering networks in the first place
- Keep them from finding data
- Keep them from getting data out
- Detect and respond to incidents in a timely and effective manner

You can be prepared:

- PCI DSS Compliance
- Layer Security
- Investigation Response Program

