Powerful Insights.
Proven Delivery.™

Cybersecurity Threats and Industry Response

Presented by:
Mark Lippman
Managing Director
February 13, 2014

protiviti®
Risk & Business Consulting.
Internal Audit.

Speaker

Presenter	**Mark Lippman** Managing Director
Topic	Cybersecurity Threats and Industry Response
Objective	Provide: • An overview of key Cybersecurity risks • How companies can protect themselves
Relevant Experience	• Managing Director in Security & Privacy Practice • Formerly CEO and co-founder of Arsenal Security Group which was acquired by Protiviti in June 2012 • 15 years of IT Security consulting experiences focused on Payment Card Industry (PCI) including 7 years at IBM

protiviti®

Why do we care?

Pulled from the Headlines:

- ✓ 563 Million Sensitive Records Breached Since 2005
- ✓ Malicious data breach cases averaged to $222 per record, with malicious attaches being the most expensive cause of data breaches and on the rise.
- ✓ Negligence accounted for 39 percent of reported breaches.
- ✓ The number of identities exposed during 2011 totaled to more than 232.4 million.
- ✓ In the first half of 2013 there were219 incidents, exposing 8,525,746 records.

And the list continues……

protiviti®

protiviti®

What is the corporate risk?

The risks are more than just immediate monetary impact:

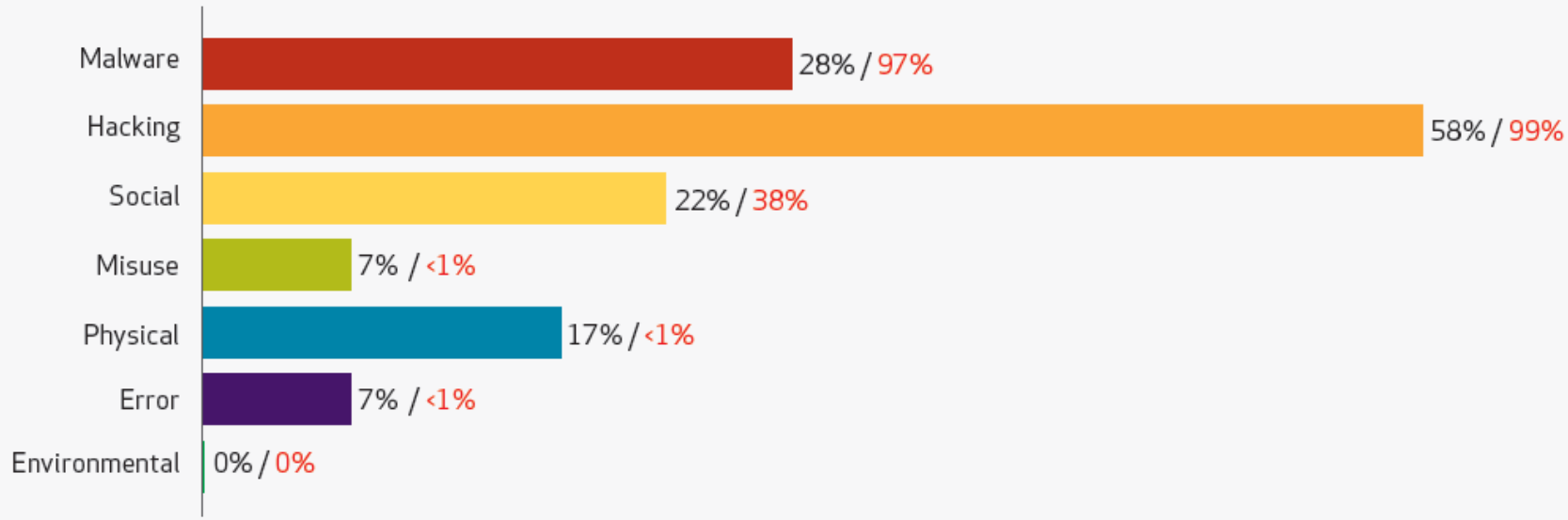
- ✓ Litigation
- ✓ Reputation Loss
- ✓ Loss of System Availability
- ✓ Lost Productivity
- ✓ Loss of Intellectual Property
- ✓ Regulatory Fines

protiviti®

Threats

Summary of Threat Agents (Verizon Data Breach Report 2012)

Malware and Hacking account for most breached records



protiviti®

Who's to Blame?

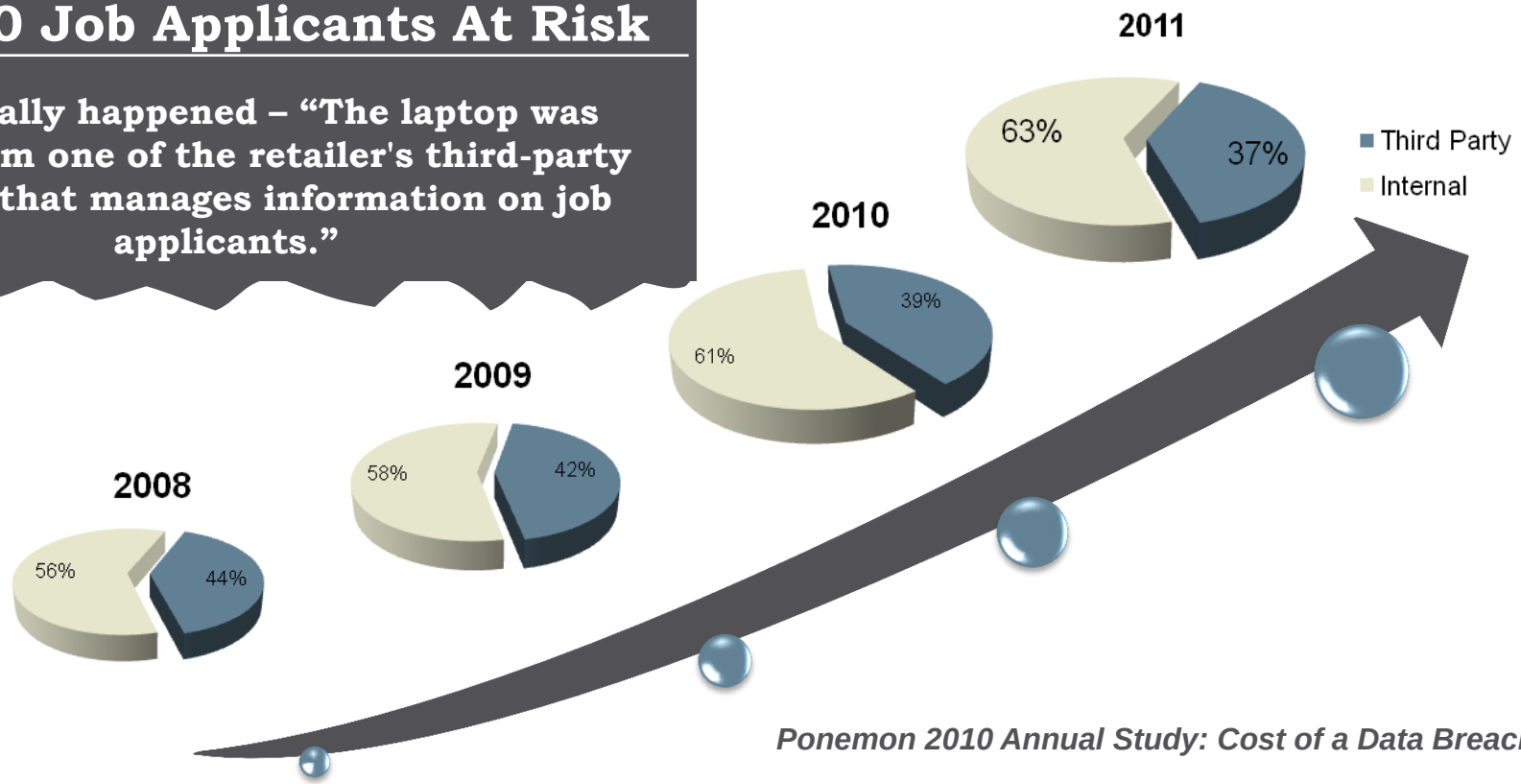
Final Edition

Source: Information Week, October 2007

Headline News

Theft Of Gap Laptop Puts 800,000 Job Applicants At Risk

What really happened – "The laptop was stolen from one of the retailer's third-party vendors that manages information on job applicants."



Ponemon 2010 Annual Study: Cost of a Data Breach

protiviti®

Information security

With security breaches being an every day event, regulators remain very focused on:

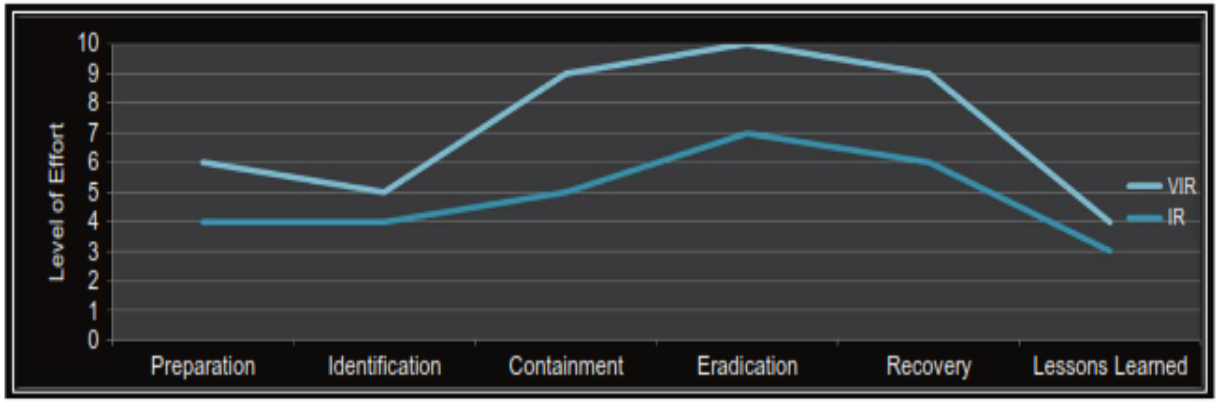
- **Vendor Management**
  - What roles do third parties play in supporting the company's technology needs?
- **Emerging Technologies**
  - **Cloud**
  - **Mobile**
- **Data governance and data leakage prevention (DLP)**
- **Application security**
  - Are Security Development Lifecycle protocols embedded in the application development process?
  - Are periodic pen tests performed to identify vulnerabilities?
- **Database Security**
- **Social Engineering**
- **Incident Response**
  - Are there well-defined and communicated processes in place to respond to security breaches?

protiviti®

Information security – vendor management

Vendors are a common source of data loss and incidents, as such companies are increasingly faced with more due diligence in managing profiles, completing risk assessments, streamlining management, and reporting key metrics:

- Limited visibility
- Limited resiliency
- Limited responsibility
- Increased data exposure
- Increased regulatory exposure



protiviti®

Information Security – emerging risks

As mobile devices gain popularity and are used throughout businesses, new risks emerge:

- Business data stored on personal mobile devices
- Lost mobile devices
- Insecure Apps
- Malware
- Misconfiguration

Many companies are not prepared to handle mobile device loss and may lack policies and response procedures to be prepared.

protiviti®

Information Security – emerging risks

Companies are processing and storing data in the "cloud" and this creates new challenges:

protiviti®

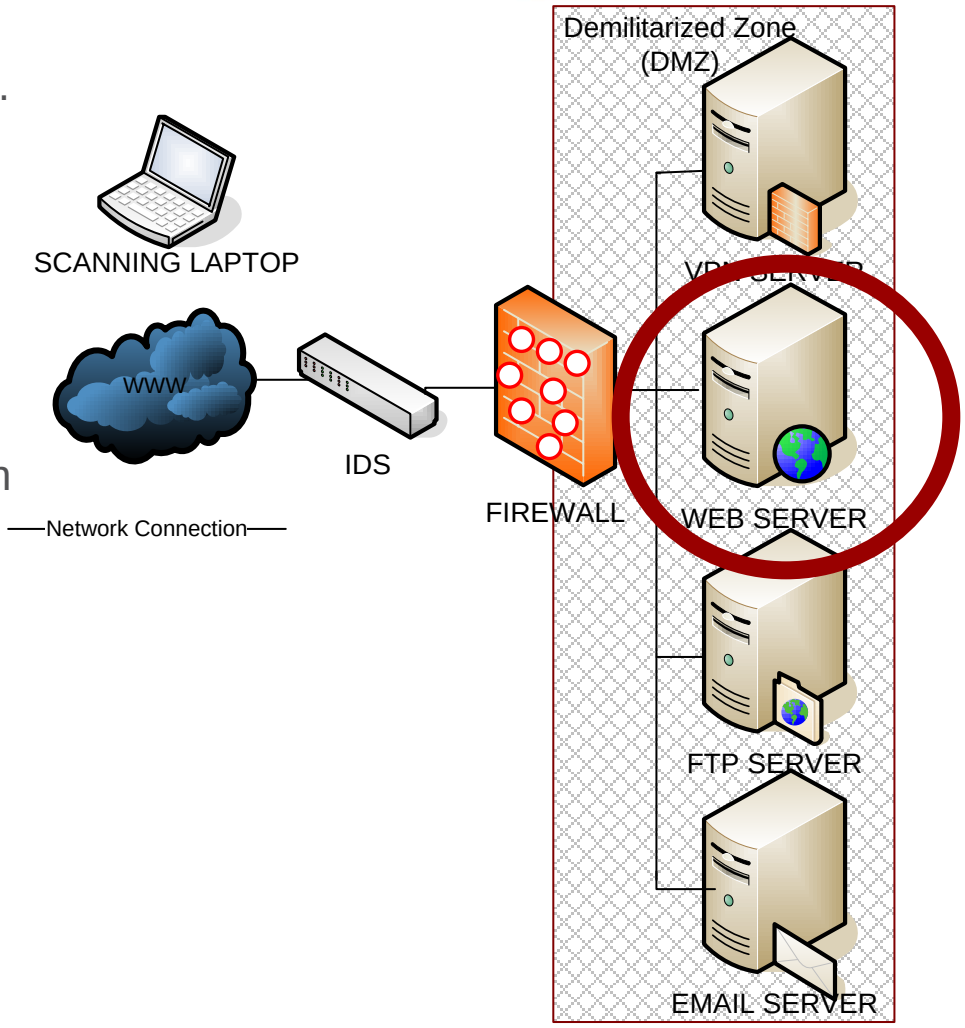
Web Application Issues

- Verizon 2012 Data Breach Investigative Report (DBIR)
  - Web App related vulnerabilities:
    - 10% of all hacking breaches
    - **54% for larger organizations** (employees greater than 1000)
- (In)Famous Data Breaches
  - **Heartland Payment Systems**, March 2008, (SQL Injection)
    - Compromise of 130 million credit and debit card numbers
  - **Citi**, May 2011 (Weak Session Management, Access Control)
    - Compromise of 1% of credit card accounts, 360,069 accounts
  - **HBGary Federal**, 2011, (SQL Injection) exposes 60,000 confidential emails, executive social media accounts, and customer information
  - **Sony**, 2011, (Outdated Apache Software) exposes 100 million customer account details and 12 million unencrypted CC

protiviti®

What About the Web Applications?

- 75% of web site hacks that occur today happen at the application level (Gartner).
- Firewalls and most Intrusion Detection Systems (IDS) sit at the network layer and typically do not protect the application layer.
- Threats still exist through the exploitation of the way the application is designed and programmed.
- On average, there are 5 to 15 defects in every 1,000 lines of code (US Dept. of Defense and the Software Engineering Institute).



protiviti®

Database Security

Where are your valuables?

- Is it your data, systems, or network?
- Current focus is towards protecting information through network configuration, systems administration, application security
- How about the data in the database and the systems that manage it?

Security in Layers:

- Secure database
- Secure applications
- Secure operating system (relative to database system)
- Secure web server (relative to database system)
- Secure network environment (relative to database system)

The database security is often a neglected area because it is typically not well understood by DBA's and auditors

protiviti®

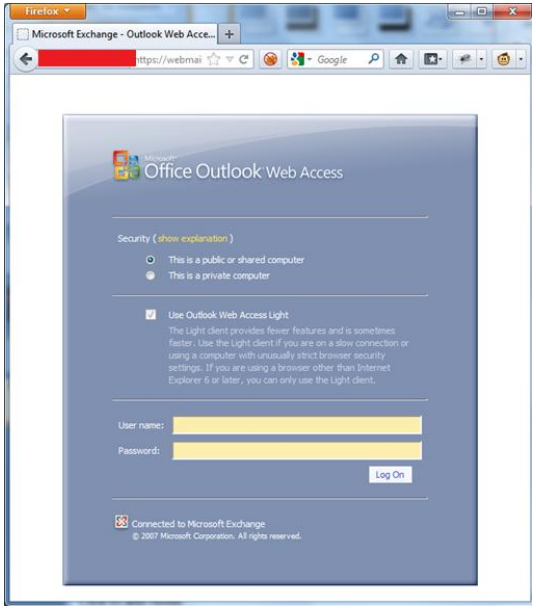
Common Database Security Findings

- Weak user account settings - Databases lack user settings found in more mature operating system.
- Insufficient segregation of duties
- Inadequate audit trails .
- Unused database security features
- Access management/user administration/IDM is often an issue - User account reconciliation or review does not occur.
- - Related to "Insufficient segregation of duties" - Applications are often connecting to the DB using accounts that are more powerful then they need to be or have resources to much more then the really need to.

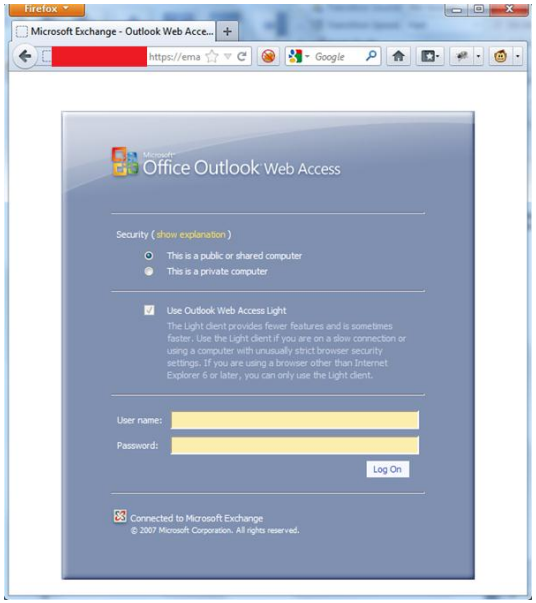
protiviti®

Social Engineering

Can you tell them apart?



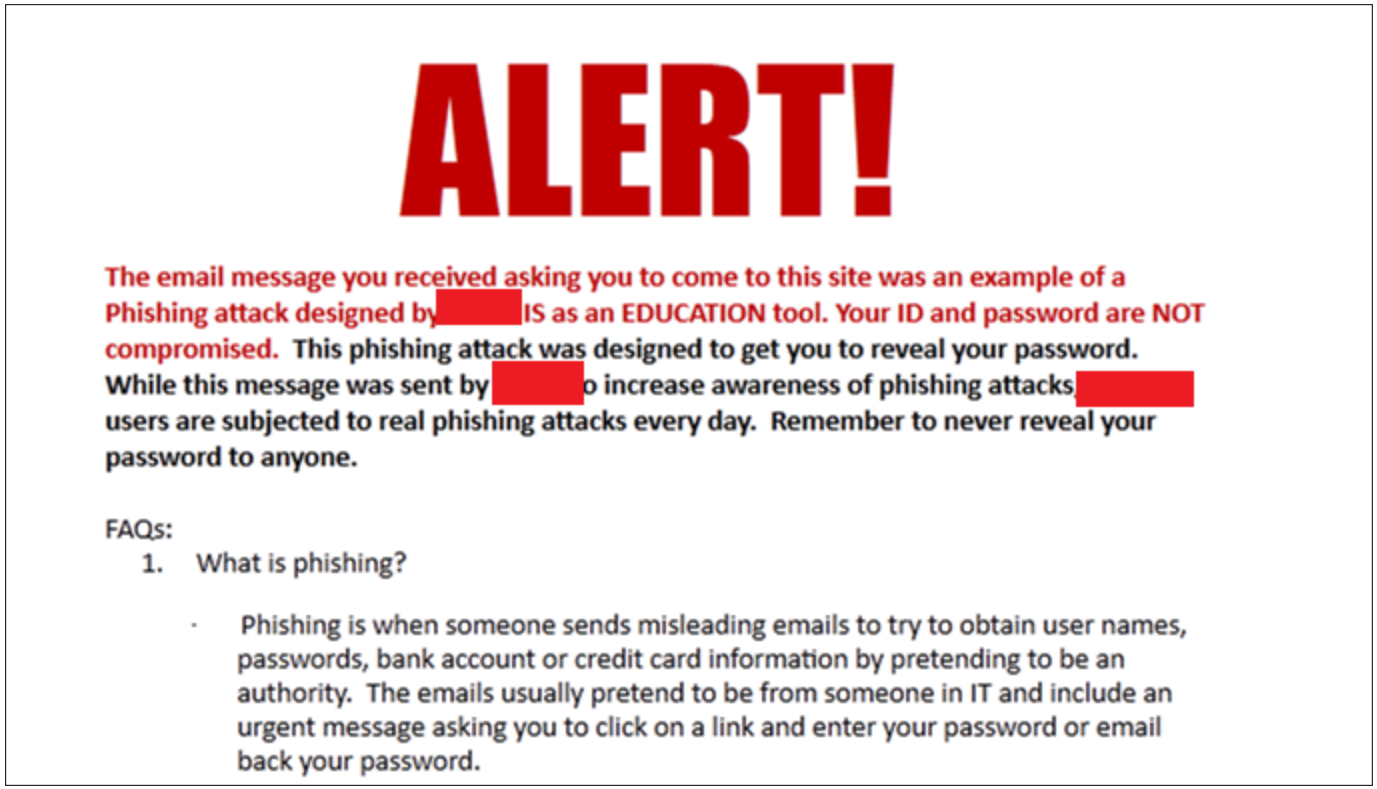
Customer's Outlook Web



Phishing Site

protiviti®

Phishing as Security Awareness Tool



ALERT!

The email message you received asking you to come to this site was an example of a Phishing attack designed by [redacted] IS as an EDUCATION tool. Your ID and password are NOT compromised. This phishing attack was designed to get you to reveal your password. While this message was sent by [redacted] o increase awareness of phishing attacks [redacted] users are subjected to real phishing attacks every day. Remember to never reveal your password to anyone.

FAQs:

1. What is phishing?

   - Phishing is when someone sends misleading emails to try to obtain user names, passwords, bank account or credit card information by pretending to be an authority. The emails usually pretend to be from someone in IT and include an urgent message asking you to click on a link and enter your password or email back your password.

protiviti®

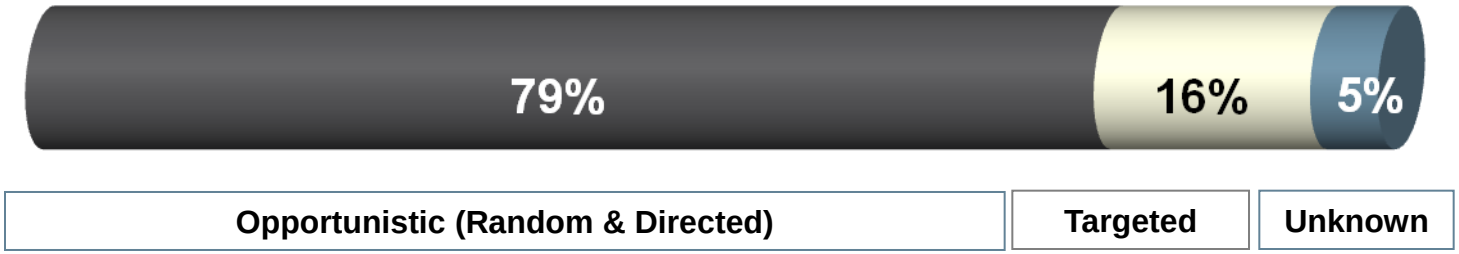
Incident Response Statistics

***75%** of breaches are **executed within minutes** of initial internal network access

***54%** of the time, it takes organizations **more than one month to become aware** of a compromise

***92%** of organizations are made aware of a breach because of **third party notification**

***38%** of organizations take **longer than one week to respond and mitigate** a breach

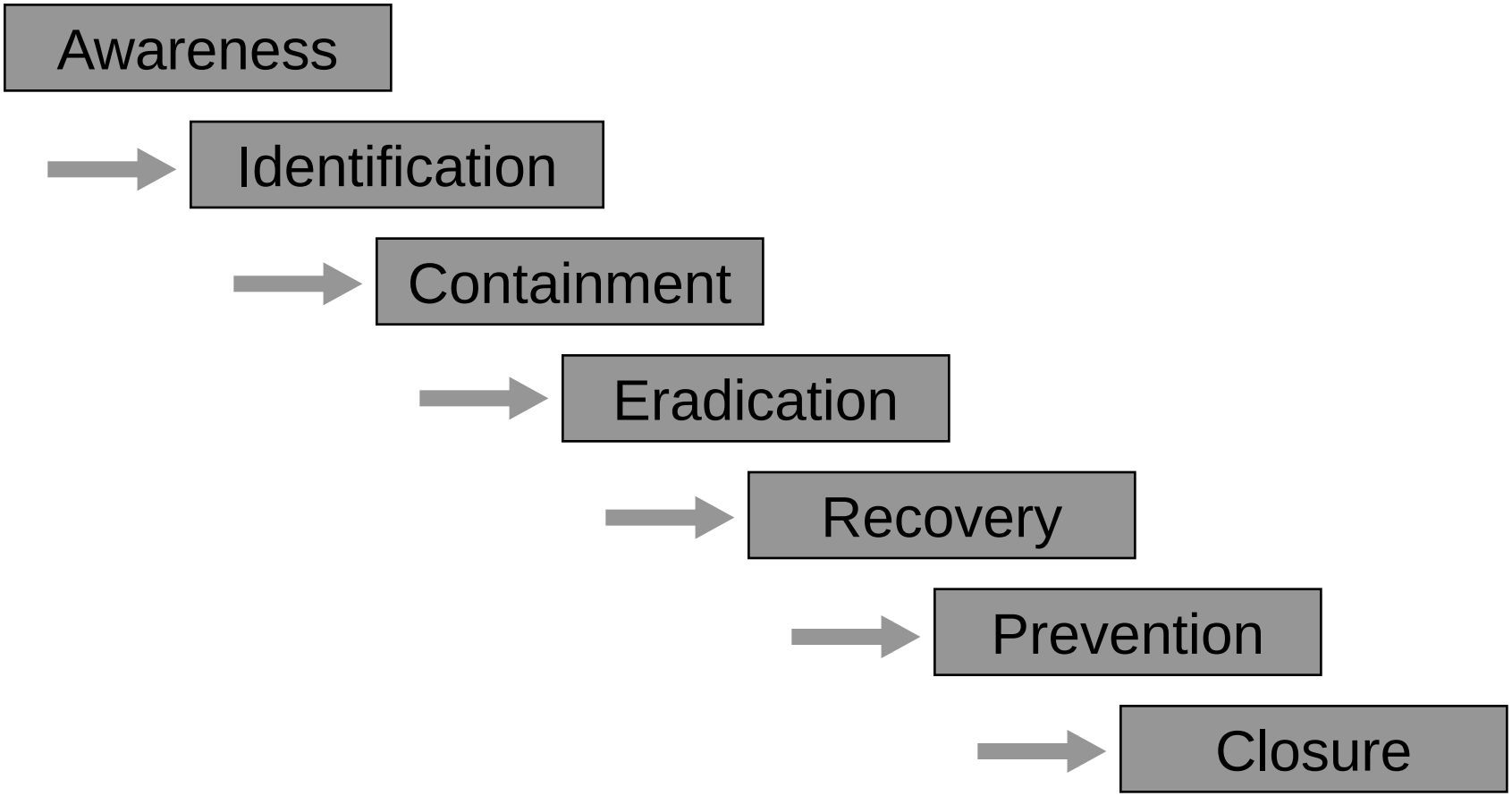


Verizon Data Breach Investigations: Supplemental Report

***By percent of breaches for all organizations**

protiviti®

Incident Response Process Architecture



protiviti®

Incident Response

Throughout the response process the following are key:

- Communication – Who, What, Where, and When
  - ✓ Regulatory considerations – SB1386 and others
  - ✓ Consider communication channels within and outside the organization
- Chain of Custody
- Documentation – Record and log actions
  - ✓ Develop and use incident handling forms
- Collect data that can be used to quantify damage

protiviti®

Mitigation Trends

After a data breach, organizations are relying on a combination of **people-centric** and **technology-centric** based steps. One technique not depicting is Breach insurance which we are seeing become more popular.

Preventative Measure	2011	2010	2009
Training and awareness programs	53%	63%	67%
Expanded use of encryption	52%	61%	58%
Additional manual procedures and controls	49%	54%	58%
Identity and access management solutions	47%	52%	49%
Data loss prevention (DLP) solutions	45%	43%	42%
Other system control practices	38%	43%	40%
Endpoint security solutions	42%	41%	36%
Security certification or audit	19%	29%	33%
Strengthening of perimeter controls	25%	22%	20%
Security event management systems	26%	21%	22%

Ponemon 2011 Annual Study: Cost of a Data Breach

protiviti®

Goals of IT Risk Assessment and Management

- Accurate view on current and near-future IT-related events
- End-to-end guidance on how to manage IT-related risks
- Understanding of how to capitalize on the investment made in an IT internal control system already in place
- Integration with the overall risk and compliance structures within the enterprise
- Common language to help manage the relationships
- Promotion of risk ownership throughout the organization
- Complete risk profile to better understand risk

protiviti®

How do you get there?

Plan

- Formalize a plan for Information Risk Management
- Identify Stakeholders and Obtain Support

Execute

- Select a Risk Management Framework
- Ensure a Comprehensive Approach and Scope

Monitor

- Complete Assessment with Risk Outcomes
- Identify Ownership, Manage, Report, and Assess Mitigation

protiviti®

Example of a Risk Management Framework: ISO 27001

(Information technology – Security techniques – Information security management systems – Requirements)

Security Policy

- Information Security Policy

Organization of Information Security (Organizational Security)

- Manage information security within the Company
- Information Security Infrastructure
- Security of Third Party Access
- Outsourcing

Asset Management (Asset Classification and Control)

- Accountability for Assets
- Information Classification

Human Resource Security (Personnel Security)

- Security in Job Definition and Resourcing
- User Training
- Responding to Security Incidents and Malfunctions

Physical and Environment Security

- Secure Areas
- Equipment Security
- General Controls

Communications and Operational Management

- Operational Procedures and Responsibilities
- System Planning and Acceptance
- Protection Against Malicious Software
- Housekeeping
- Network Management
- Media Handling and Security
- Exchanges of Information and Software

Access Control

- Business Requirement for Access Control
- User Access Mgmt
- User Responsibilities
- Network Access Control
- Operating system access control
- Application Access Control
- Monitoring system access and use
- Mobile Computing and Tele-working

Systems Development and Maintenance

- Security Requirements of Systems
- Security in Application Systems
- Cryptographic Controls
- Security of System Files
- Security in the development and support processes

Information Security and Incident Management

- Incident Detection
- Incident Reponses
- Incident Escalation

Business Continuity Management

- Aspects of Business Continuity Management

Compliance

- Compliance with legal requirements
- Review of Security Policy and Tech controls
- System Audit Considerations

protiviti®

PCI Data Security Standard:

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

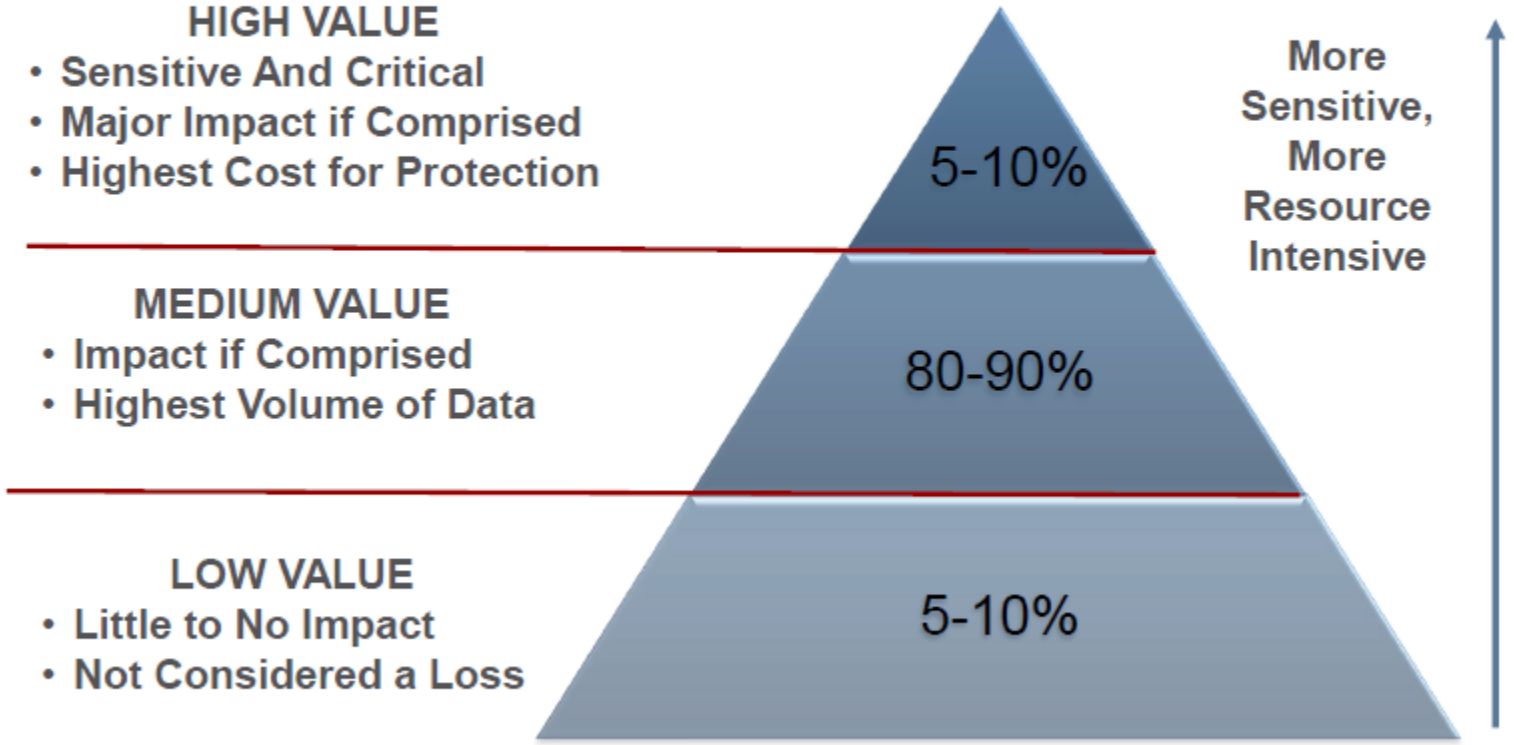
protiviti®

Data Sensitivity and What It Means

HIGH VALUE
- Sensitive And Critical
- Major Impact if Comprised
- Highest Cost for Protection

MEDIUM VALUE
- Impact if Comprised
- Highest Volume of Data

LOW VALUE
- Little to No Impact
- Not Considered a Loss



protiviti®

Risk Assessment Metrics

Risk Calculation

Impact Severity * Occurrence Likelihood = Inherent Risk – Safeguards (Controls) = Residual Risk

Asset Valuation

Assets are defined as a system or applications used to store, process or transmit client data. Specific asset categories are to be discussed and agreed upon in the beginning stages of the review.

Impact Severity

Impact severity is the measure of the effect, vulnerability will have on an asset when exercised by a threat. For the Risk Assessment, impact severity was defined by the amount of cardholder data and sources likely to be exposed.

Occurrence Likelihood

This is the estimated probability that a threat will occur for a given asset.

Risk Calculation

Inherent risk was calculated as high, medium or low by cross indexing the metric factors for impact severity and likelihood of occurrence on the table below. This table was calibrated to represent the total reputational and financial risks presented to client by the threat vulnerability asset pairings in the SRA tool.

Safeguards

The technical, procedural, or physical measures in place that protect an asset from risk.

Residual Risk

Residual risk is calculated as high, medium or low based on the highest risk individually assessed threat, vulnerability and safeguard combination. The risk rating for the TVS combination is based on the revised likelihood and severity calculation, accounting for the effect of an applied safeguard. The metrics are adapted from NIST and other leading methodologies as well as input from client management regarding quantitative scale metrics. For each asset, threat, vulnerability and safeguard combinations are assessed for residual risk. The totality of TVS combinations is assessed with consideration for the data affected.

protiviti®

Summary

- Corporate assets continue to be targeted for malicious intent
- The expansion of IT assets (devices and data) makes protection of assets more challenging
- Non- IT (Finance, Internal Audit, Line of Business) play a critical role in assuring controls are in place.

protiviti®

Resources

Web Sites:

- ✓ Protiviti www.protiviti.com
- ✓ National Institute of Standards and Technology (NIST) http://csrc.nist.gov/
- ✓ SANS http://www.sans.org/resources/
- ✓ CERT Coordination Center http://www.cert.org/other_sources/
- ✓ Privacy Rights Clearinghouse www.privacyrights.org
- ✓ In Defense of Data www.indefenseofdata.com

Incident Response Resources

- ✓ United States Computer Emergency Readiness Team http://www.us-cert.gov
- ✓ NIST Computer Security Resource Center http://csrc.nist.gov
- ✓ SANS Institute http://www.sans.org
- ✓ Computer Emergency Response Team (CERT) http://www.cert.org

protiviti®

Thank You

Mark Lippman
Managing Director
Tysons Corner, VA
+1 703-980-8715
Mark.lippman@protiviti.com

29

protiviti®

Powerful Insights.
Proven Delivery.™

protiviti®