Creating, Developing and Instituting an Effective Incident Response Plan

Webinar

15 April 2015

Stan Hui – Payment System Security
Stephen J. Kopeck – Verizon

Disclaimer

The information or recommendations contained herein are provided "AS IS" and intended for informational purposes only and should not be relied upon for operational, marketing, legal, technical, tax, financial or other advice. When implementing any new strategy or practice, you should consult with your legal counsel to determine what laws and regulations may apply to your specific circumstances. The actual costs, savings and benefits of any recommendations or programs may vary based upon your specific business needs and program requirements. By their nature, recommendations are not guarantees of future performance or results and are subject to risks, uncertainties and assumptions that are difficult to predict or quantify. Assumptions were made by us in light of our experience and our perceptions of historical trends, current conditions and expected future developments and other factors that we believe are appropriate under the circumstance. Recommendations are subject to risks and uncertainties, which may cause actual and future results and trends to differ materially from the assumptions or recommendations. Visa is not responsible for your use of the information contained herein (including errors, omissions, inaccuracy or non-timeliness of any kind) or any assumptions or conclusions you might draw from its use. Visa makes no warranty, express or implied, and explicitly disclaims the warranties of merchantability and fitness for a particular purpose, any warranty of non-infringement of any third party's intellectual property rights, any warranty that the information will meet the requirements of a client, or any warranty that the information is updated and will be error free. To the extent permitted by applicable law, Visa shall not be liable to a client or any third party for any damages under any theory of law, including, without limitation, any special, consequential, incidental or punitive damages, nor any damages for loss of business profits, business interruption, loss of business information, or other monetary loss, even if advised of the possibility of such damages.

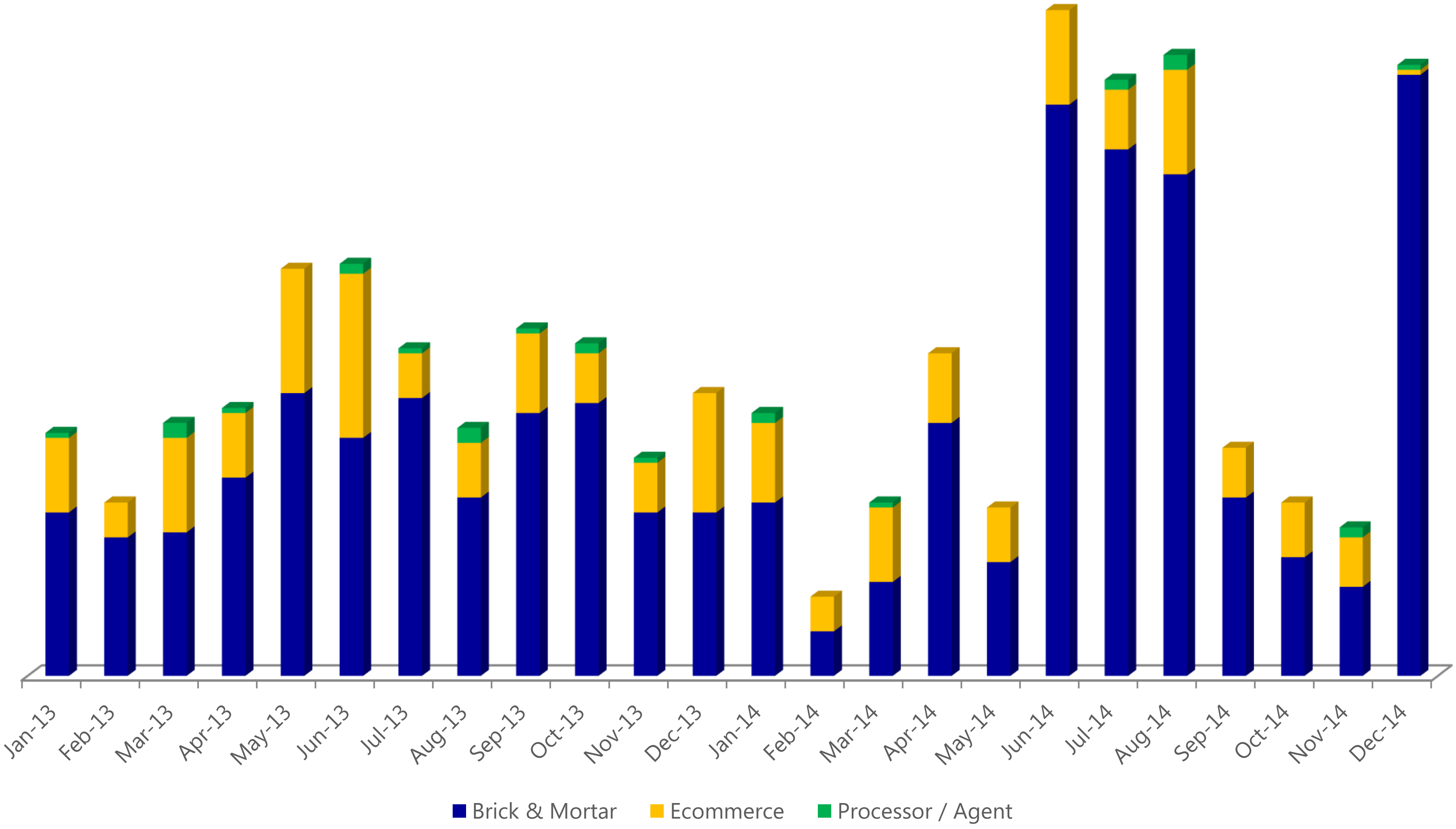
Agenda

- Data Breach Landscape
- The Need for Incident Response
- Incident Response Plan Elements
- Questions and Answers

Data Breach Landscape

Stan Hui

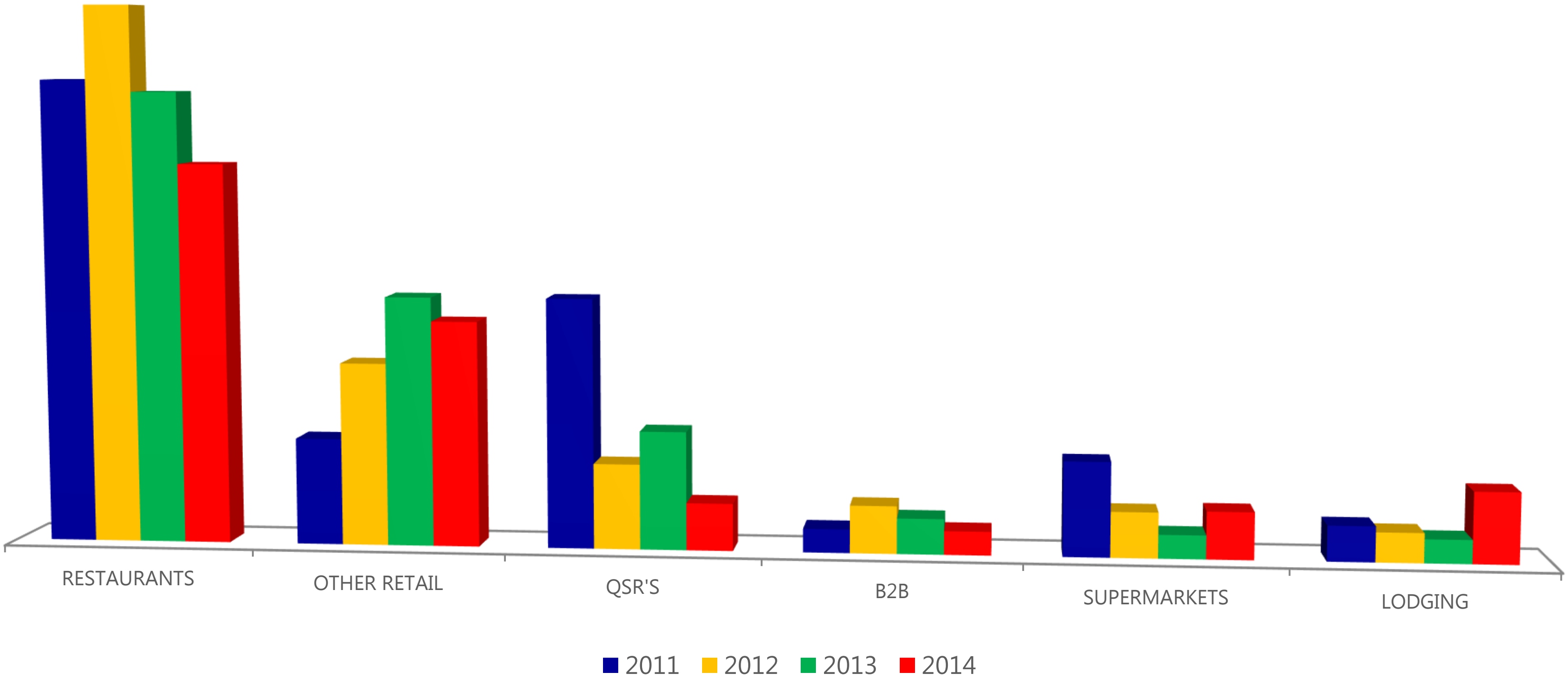
Visa Inc. CAMS Compromise Events
Entity Type by Month



Source: Compromised Account Management System (CAMS) – Original "IC" and "PA" Alerts

Visa Inc. CAMS Compromise Events
Top Market Segment* (MCC)

- Restaurants and retailers are leading market segments in 2014
- Insecure remote access and poor credential management continue to be attack vectors



* Market Segment based on Acceptance Solutions MCC "Market Segment" category

Source: Compromised Account Management System (CAMS) – Original "IC" and "PA" Alerts

Recent Threats due to POS Integrators

- POS Integrators support merchant POS software installations
- Typically merchant setup includes Remote Access Services (RAS) for monitoring and software support
- Integrators have access to POS system - however PCI compliance not maintained
- Multiple POS Integrator related compromises since June 2014
- Merchants infected with ‘Backoff’ family of malware
- Remote Access Services and Applications Exploited
  - Currently **LogMeIn** users targeted (other RAS include: Remote Desktop Protocol, PCAnywhere, TeamViewer and VNC)
  - Brute forces login credentials
  - Creates a ‘backdoor’, logs keystrokes and collects credit card data
  - Extremely low anti-virus detection rates
  - Exfiltration to remote IP addresses
- Non-Compliant Integrators / Merchants set up with default / shared remote access IDs without two-factor authentication or regular password changes
  - Entities not following PCI compliant practices

Merchant Due Diligence

Requirement 12 – Maintain a policy that addresses information security for all personnel

- Requirement 12.5.3 – Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations
- Requirement 12.10 – Implement an incident response plan. Be prepared to respond immediately to a system breach

"Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities."

- Requirement 12.10.1 – Create the incident response plan to be implemented in the event of system breach

Creating, Developing and Instituting an Effective Incident Response Plan

Stephen J. Kopeck, Verizon

verizon
RISK Team

VISA

PROPRIETARY STATEMENT

This document and any attached materials are the sole property of Verizon and are not to be used by you other than to evaluate Verizon's service.

This document and any attached materials are not to be disseminated, distributed, or otherwise conveyed throughout your organization to employees without a need for this information or to any third parties without the express written permission of Verizon.

OBJECTIVE

OBJECTIVE—

To outline and discuss the fundamental components of developing, and implementing an Incident Response Plan.

PUTTING IT INTO PERSPECTIVE

THE NEED FOR IR—

- **Incidents continue to occur with increasingly sophisticated threats:**
  - organized crime / sensitive data theft
  - denial of service attacks / “hacktivism”
  - insider threats / corporate espionage
  - malware outbreaks
- **Question of not “if”, but “when”**
- **Solution = IR Plan**

IR is not just an IT problem…

- Management
- Legal
- Human Resources
- Physical Security
- Loss Prevention
- Corporate Communications
- Others, as necessary

The cost of being prepared is always less than being a victim

PUTTING IT INTO PERSPECTIVE

THE NEED FOR IR—

1 – Recover quickly from an incident

—damage and loss minimized

—future incidents prevented, or at least mitigated

2 – Implement a pre-planned strategy

—efficient, effective, and repeatable process

3 – Protect the company's interests

—proprietary information / intellectual property

—sensitive customer data

—brand image / reputation

4 – Maintain compliance

—legal liability reduced

—insurance costs reduced

IR Plan Elements

FOCUS AREAS—

—Scope & Purpose

—IR Roles and Responsibilities

—Internal Stakeholders

—External Entities

—IR Process Flow/Phases

—Revision History

—IR Resources

—IR Stakeholder Contact List

—First Responder Checklist

—Incident Report Template

—Evidence Chain of Custody/Log

IR Plan - Stakeholders

INCIDENT RESPONSE STAKEHOLDERS—

—Chief Information Risk Officer

—Incident Response Team / Manager

—Business Organizations / Managers

—Information Technology (IT) Organizations / Managers

—Information Security / Officers

—Legal

—Human Resources

—Compliance

—Physical Security

—Loss Prevention

—Corporate Communications / Public Relations

It ultimately depends on the situation…

INCIDENT RESPONSE ELEMENTS

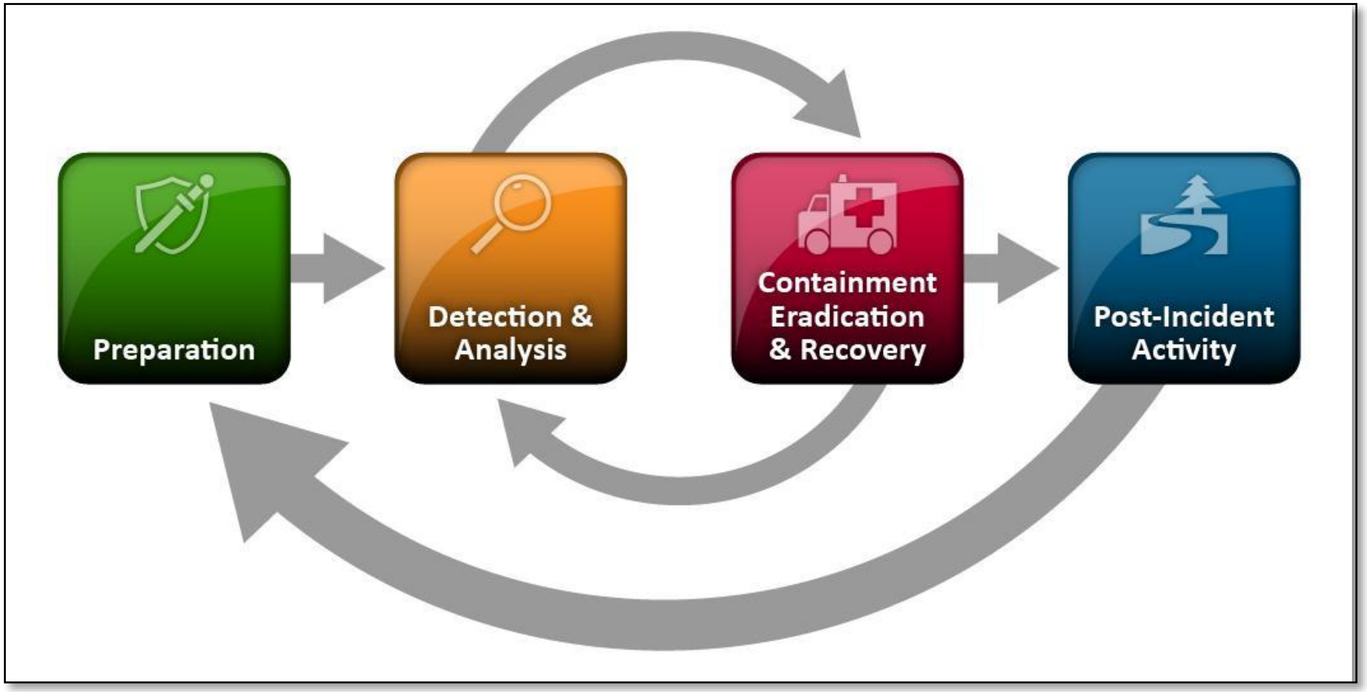
INCIDENT RESPONSE PHASES—

- Preparation
- Detection & Analysis
- Containment, Eradication, & Recovery
- Post-Incident Activities

NIST SP 800-61, R2, Computer Security Incident Handling Guide

INCIDENT HANDLING ELEMENTS

INCIDENT RESPONSE PROCESS—



Source: NIST SP 800-61, R2, Computer Security Incident Handling Guide

RECOMMENDATIONS

THINGS TO CONSIDER—

- Less is more philosophy
- Develop, Review, Train, & Operate by the Plan
- It is a living document
- Ensure everyone is familiar with the plan – Required reading

CONCLUSION

TAKE-AWAYS—

- Remember any organization can be a target
- Establish policies and plans before an incident occurs
- Processes should be reliable and consistent
- Ensure Incident Responders are trained and know their roles, responsibilities, & authorizations
- Maintain good documentation
- Always consider preservation of evidence
- Engage outside help if necessary; don’t exceed your knowledge level
- Ensure maximum participation in post-mortem discussions; integrate lessons-learned into Incident Response Plan

The cost of being prepared is far less than being a victim

VISA

2015 Visa Payment Security Symposium

The Power of Partnership

Securing the Future of
Commerce Together

August 12-13, 2015
Hyatt Regency Hotel
Burlingame, CA

Visa is hosting a must-attend event that will focus on trends and developments related to cyber security, mobile payments, e-commerce and Visa's global authentication strategy. In order to secure the future of commerce all stakeholders including merchants, acquirers, agents and Visa need to collaborate on key initiatives in addressing today's most relevant issues. This event will be held in the San Francisco Bay Area at the Hyatt Regency Hotel just south of San Francisco. For more information, email pcirocs@visa.com.

Upcoming Merchant Events and Resources

Upcoming Webinars – Training tab on www.visa.com/cisp

- Identifying and Mitigating Threats to E-commerce Payment Processing
  - 29 April 2015, 10 am PST
- Strategies to Effectively Manage Data Compromise Events
  - 27 May 2015, 10 am PST

Visa Data Security Website – www.visa.com/cisp

- “What To Do If Compromised” Guidelines
- Alerts, Bulletins
- Best Practices, White Papers
- Webinars

PCI Security Standards Council Website – www.pcissc.org

- Data Security Standards – PCI DSS, PA-DSS, PTS
- Programs – ASV, ISA, PA-QSA, PFI, PTS, QSA, QIR, PCIP, and P2PE
- Fact Sheets – ATM Security, Mobile Payments Acceptance, Tokenization, Cloud Computing, and many more…

STEVE KOPECK
PRINCIPAL CONSULTANT | VERIZON RISK
STEPHEN.KOPECK@VERIZON.COM
202.384.2687