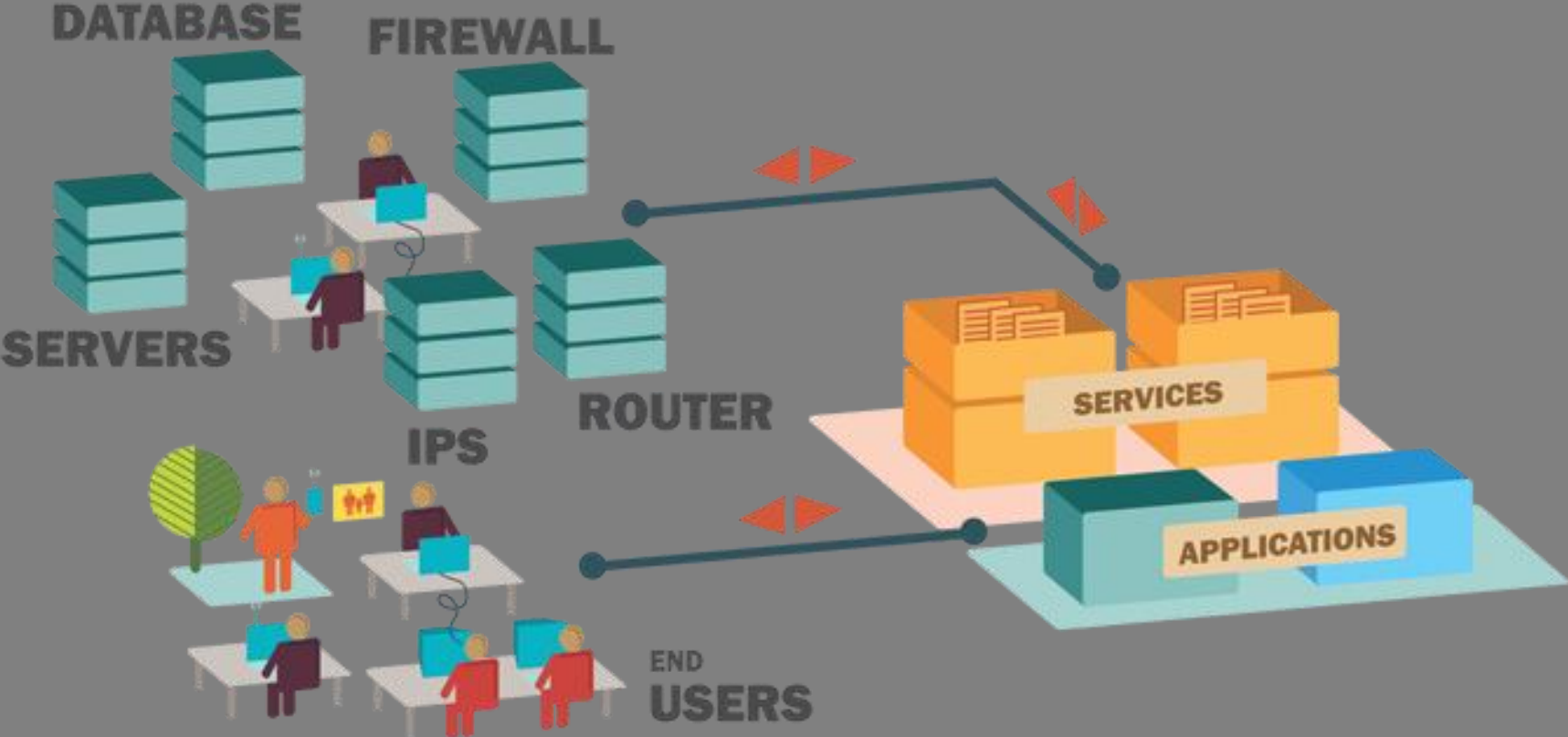


Pillars of Incident Response: The Calm in the Storm

Brandie Anderson

Senior Manager, Global Cyber Security Production Management
Hewlett-Packard

Understand Yourself and Your Organization



SITREP – Breach Setup

The 19 Days of TARGET

November 2013



Eastern Time Time Zone

Page 2/2

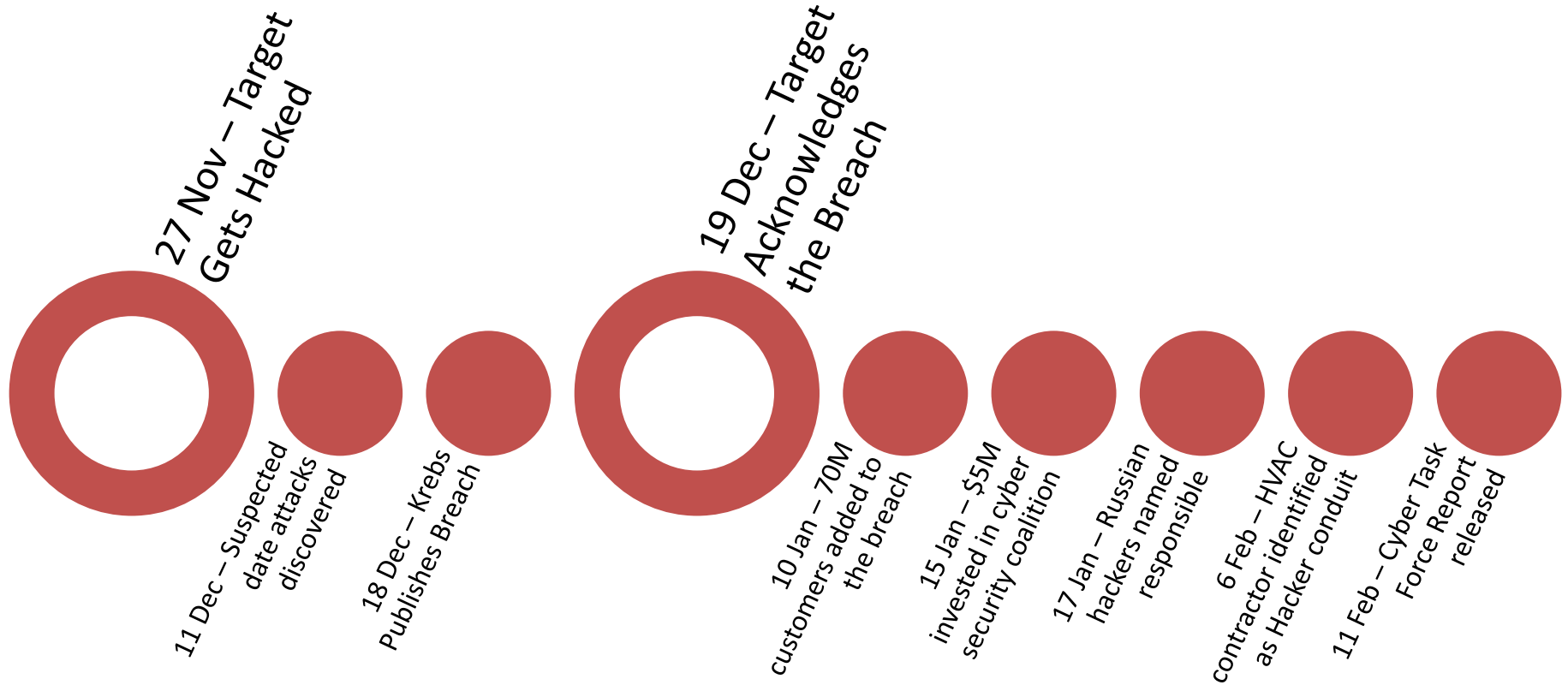
December 2013



Eastern Time Time Zone

Page 2/2

Timeline of Breach



4 Interesting Days

Dec 11 – Dec 15



Preparation



Identification



Containment

Beyond the first 4 Days



Eradication

Recovery

Lessons
Learned

Trust in Your Training



Training or Experience?



Decisions



Communication

eBay and PP sites breached

Whitted, Paul



To: Moody, Lucas

Cc: Black, Paul; Nguyen, Viet (NetSec); West, Scott; Fang, Michelle; Forsythe, Ralph
; Patino, Juan; Stuart, Robin; Stidham, Keith; DL-Ebay-TDO-Staff@ebay.com;
DL-PP-M-NOC-Group; DL-PP-M-NOC-TDO; DL-PP-dns;

Saturday, February 01, 2014 12:05 PM

Just pointing out if someone has remote access to email via compromised laptop and is on this thread then they now have our conference info to listen into this incident. Might want to have folks call into the sec / ppcc and be in breakout where password is required to join.

Paul

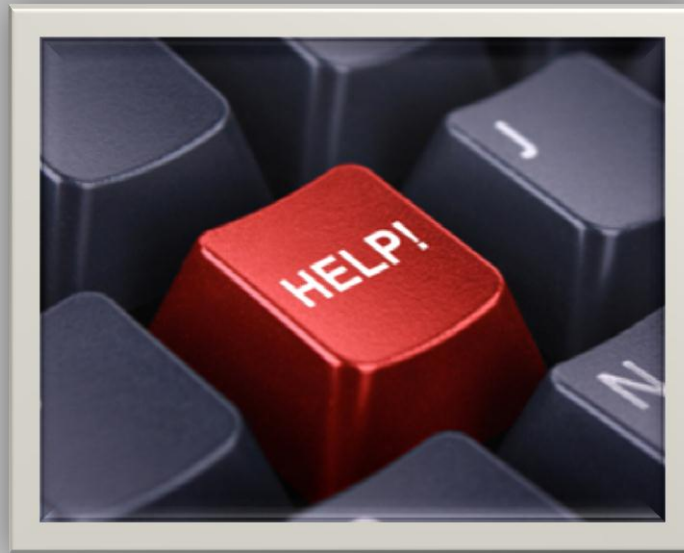
Sent from my iPhone

Critical Input



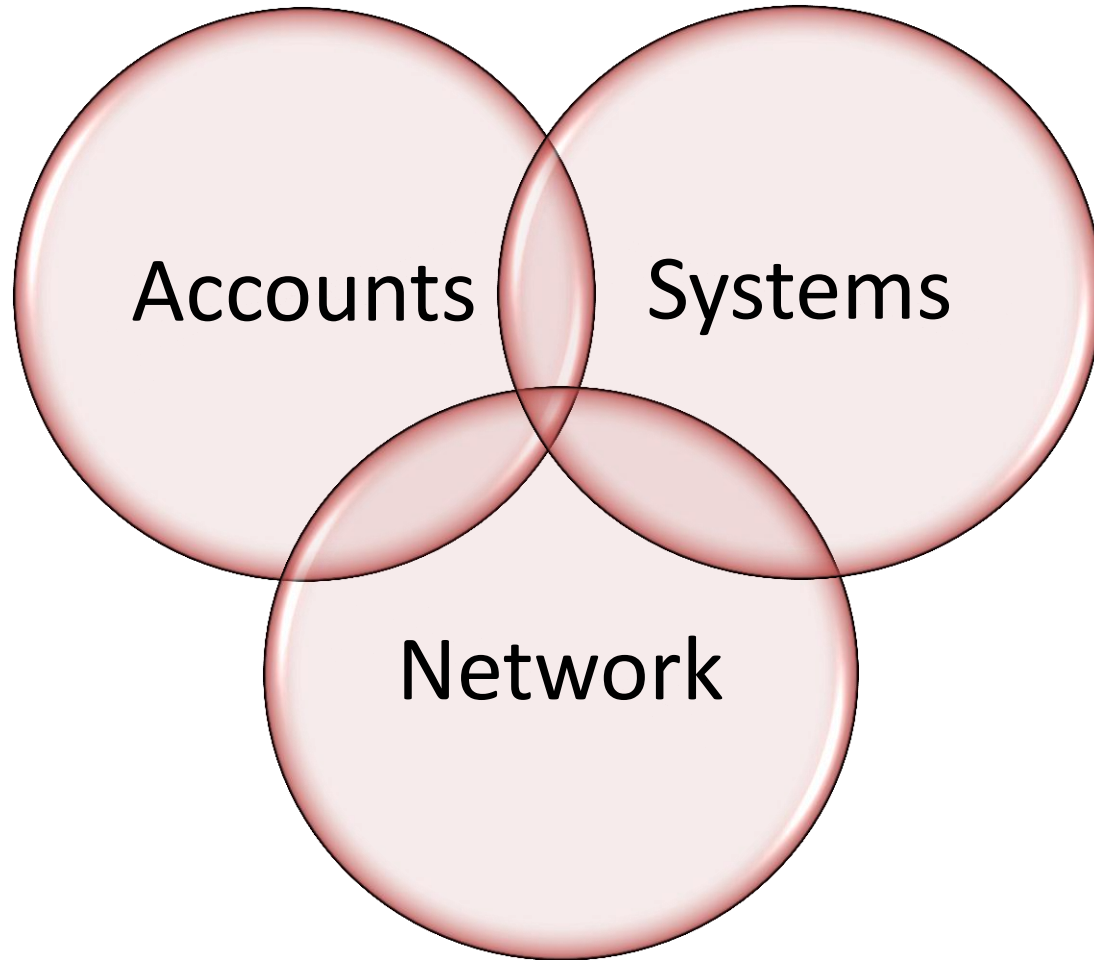
Remediation

Short Term



Long Term

Fundamentals



Get Help



Resources


Investigators



Forensics

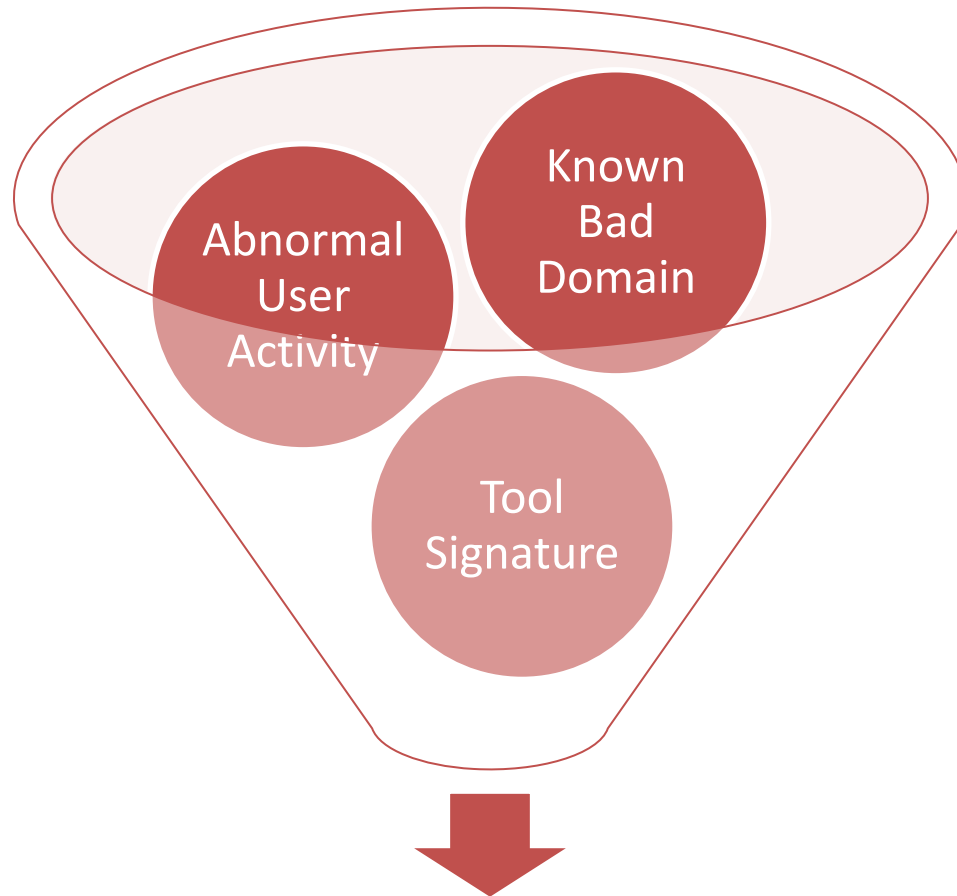


IT



Follow Up!

Remediation Validation



Actionable Data

Fall Out



briankrebs

@briankrebs

What good is a "communications hotline" if nobody answers the phone or calls you back? Sigh

1/31/2014 10:06:24 AM

3 RETWEETS 4 FAVORITES



Wrap Up



Understand
Yourself & Your
Organization

Trust Your
Training

Get Help

Thank You



@ba2trinity