Evolving role of PSIRT in the Cloud

Vic Chung, SAP
March 2, 2017
### Shipment Documents

<table>
<thead>
<tr>
<th>Shipment</th>
<th>Delivery</th>
<th>MultiDeliv</th>
<th>Tracking #</th>
<th>ServcAgent</th>
<th>Name 1</th>
<th>Misc Carr</th>
<th>Total Wght</th>
<th>W</th>
<th>City</th>
<th>Rg</th>
<th>Post.Code</th>
<th>Cty</th>
<th>Route</th>
<th>IncoT</th>
<th>Delivery date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2209</td>
<td>80021981</td>
<td></td>
<td>716941982</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>1,500</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/11/2011</td>
</tr>
<tr>
<td>2215</td>
<td>80021966</td>
<td></td>
<td>716941875</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>5,000</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/11/2011</td>
</tr>
<tr>
<td>2214</td>
<td>80021958</td>
<td></td>
<td>716941864</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>500</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/07/2011</td>
</tr>
<tr>
<td>2213</td>
<td>80021956</td>
<td>X</td>
<td>716941815</td>
<td>UPS</td>
<td>UPS</td>
<td></td>
<td>1</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/07/2011</td>
</tr>
<tr>
<td>2210</td>
<td>80021935</td>
<td></td>
<td>716941785</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>1</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/06/2011</td>
</tr>
<tr>
<td>2217</td>
<td>80021925</td>
<td></td>
<td>716941792</td>
<td>UPS</td>
<td>UPS</td>
<td></td>
<td>1</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/06/2011</td>
</tr>
<tr>
<td>2218</td>
<td>80021926</td>
<td></td>
<td>716941793</td>
<td>UPS</td>
<td>UPS</td>
<td></td>
<td>1</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/06/2011</td>
</tr>
<tr>
<td>2210</td>
<td>80021909</td>
<td></td>
<td>716941794</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>2</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/03/2011</td>
</tr>
<tr>
<td>2215</td>
<td>80021910</td>
<td>X</td>
<td>716941796</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>2</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/03/2011</td>
</tr>
<tr>
<td>2217</td>
<td>80021911</td>
<td></td>
<td>716941797</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>2</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/03/2011</td>
</tr>
<tr>
<td>2218</td>
<td>80021912</td>
<td></td>
<td>716941798</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>2</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>01/03/2011</td>
</tr>
<tr>
<td>2210</td>
<td>80021913</td>
<td>X</td>
<td>716941799</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>2</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>12/30/2010</td>
</tr>
<tr>
<td>2215</td>
<td>80021920</td>
<td></td>
<td>716941800</td>
<td>CNWYY</td>
<td>Con-Way Freight</td>
<td></td>
<td>2</td>
<td>LB</td>
<td>Atlanta</td>
<td>GA</td>
<td>30328</td>
<td>US</td>
<td>000001</td>
<td>FOB</td>
<td>12/30/2010</td>
</tr>
</tbody>
</table>
Purpose and Agenda

Purpose
• Share observations and host a dialog on the impact of cloud to PSIRT
• Focus on operations, not concept…the actual workings of handling vulnerabilities in real organizations
• Consider the future role of PSIRT in the Cloud (and perhaps extend to IoT?)

Proposed Agenda
• 30 minutes of presentation and sharing observations
• 15 minutes of panel discussion, share observation (solution?) where appropriate

References (just to put some structure to the discussion…without bias)
• Cloud Security Alliance
  – Security Guidance for Critical Areas of Focus in Cloud Computing v3.0
  – NIST definition of cloud (secondary reference)
  – ISO 270XX (secondary reference)
Expected outcome
So...the cloud

I know you know all about it, but just to make sure everyone is on the same page
The NIST Definition of Cloud Computing

Essential Characteristics:
- Broad Network Access
- Rapid Elasticity
- Measured Service
- On-Demand Self-Service
- Resource Pooling

Service Models:
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

Deployment Models:
- Public
- Private
- Hybrid
- Community
A fundamental shift is under way from a ‘build’ to ‘consume’ model for IT workloads.

% of companies planning to have following environments as primary environment for at least 1 workload type in 2015 and 2018

<table>
<thead>
<tr>
<th>Build</th>
<th>Consume</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traditional</td>
<td>77</td>
</tr>
<tr>
<td>Virtualized</td>
<td>43</td>
</tr>
<tr>
<td>On-premise private cloud</td>
<td>57</td>
</tr>
<tr>
<td>Dedicated private cloud</td>
<td>49</td>
</tr>
<tr>
<td>Virtual private cloud</td>
<td>49</td>
</tr>
<tr>
<td>Public IaaS¹</td>
<td>38</td>
</tr>
<tr>
<td></td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>34</td>
</tr>
<tr>
<td></td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>37</td>
</tr>
</tbody>
</table>

¹Infrastructure as a service.

Source: McKinsey IT-as-a-Service (ITaaS) Cloud Survey
The ‘cloud’


2. The ‘perimeter’

3. Supplier/Contractor problem – SLA, agreement-based

A cloud product position depends on its go-to-market strategy:

1. simple – fit in to one of the ‘cloud’ bucket

2. Or complex – with a product available in every imaginable service models and deployment models
Some standards to cloud security...


ISO/IEC 27036-x: Multipart standard for the information security of supplier relationship management that is planned to include a part relevant to the cloud supply chain

ITU-T X.ccsec: Security guideline for cloud computing in telecommunication area

ITU-T X.srfcts: Security requirements and framework of cloud-based telecommunication service environment(X.srfcts)

ISO/IEC 30111:2013 gives guidelines for how to process and resolve potential vulnerability information in a product or online service.

ISO/IEC 29147:2014 gives guidelines for the disclosure of potential vulnerabilities in products and online services.
Product in the Cyber Space

Product Incident Response – Computer (‘Cyber’) Incident Response
The pursuit of no down-time

99.99% = 4 minutes per month
99.9% = 43 minutes per month
PSIRT process abstraction

Notification as threat intelligence vs patch day model
Coordination with cloud providers, different uptime SLA
Priority based on...CVSS?
The same...perhaps cloud will attract more hackers?
More teams to deal with beyond engineering, based on vulnerability type.

- Release
- Receipt
- Triage
- Prioritize
- Patch Dev
Transition to cloud

- Hybrid product portfolio
- Patch without knowing
- Dev / IT / Ops
- Org. moving to cloud
- Short Delivery Cycle

Cloud Products
PSIRT as a sub-culture

Communications

Project Management

Security Knowledge
Our ‘real’ organization – organic growth

Context of each organization moving to the cloud is very dynamic

- Old business model (on-premise) and new business model (cloud, IoT) often co-exist
- On-premise products are converted to the cloud (or simply ‘load’ on to the cloud)
- Hybrid of models: S/P/IaaS wherever $$ is
- Internal politics, power struggle, and defined processes
- Customers demand are different – cloud customers (esp. SaaS) expect trouble-free operations and care-less of how it is managed.
- Complex partner ecosystem in the supply-chain – vulnerability notification is even more difficult
Our ‘real’ organization – M&A

Acquisition-based innovation is not new, but is very fierce among companies to race to the cloud. Does your organization face challenges when the new clashes with the old?
My Observations and Experience

1) Cloud is very agile...release management time-frame is really quick.

2) Need to patch all DC, need to make sure all DC are account for

3) Vulnerabilities discovered via institutionalized pen-test contract

4) New colleagues from M&A perceive traditional vulnerability management as history and refuse to integrate – above typical M&A resistance

5) App Sec team needs to bridge among engineering and IT, they don’t usually get along

6) How do we notify our customers of fixed vulnerabilities? There is no patch to apply...this is not easy, especially when there is a mix of cloud deployment models and simultaneous on premise/cloud product offering

7) Security Issues vs. vulnerability

8) Administration of bounty, acknowledgements
Thank you

Contact information:

Vic Chung
Product Security Architect