Security is Just Another Word without Collective Intelligence

2013

DS Benbow, VP Marketing
DS BENBOW CLIFF NOTES

- Lots of startups! (OK only 4)
- Early career: Market Analyst
# ABOUT INTERNET IDENTITY

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>Tacoma, Washington</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOUNDED</td>
<td>1996</td>
</tr>
<tr>
<td>WEBSITE</td>
<td><a href="http://www.internetidentity.com">www.internetidentity.com</a></td>
</tr>
<tr>
<td>CUSTOMER FOCUS</td>
<td>Fortune 2,000, financial services, major internet brands, defense, critical infrastructure</td>
</tr>
</tbody>
</table>
| THOUGHT LEADERSHIP | FCC: Communication, Reliability and Interoperability Council  
                      APWG: Anti-Phishing Working Group  
                      ICANN: Security and Stability Advisory Committee  
                      OTA: Online Trust Alliance  
                      FIRST: Forum of Incident Response and Security Teams  
                      MAAWG: Messaging Anti-Abuse Working Group |
Cyberattacks continue to increase in terms of sophistication, organization, and destructive impact...

“In the past 18 months, a string of highly sophisticated and targeted cyber attacks across the globe has revealed a seismic shift in the threat landscape.” 2011 RSA CISO Report

“Big Data Emerges as a Security Tool” GRT

“What's being stolen? Personal identities, money from banks, blueprints for next-generation jobs. Some estimates put the value of information hacked at up to $US400 billion every year.” Article: Almost all US networks can be hacked: Intelligence Committee

“NSA Director on Cyberattacks- ‘Everybody’s Getting Hit’” ABC News
HYPOTHESIS

• Actionable intelligence matters (not data)

• Faster intelligence equals better protection (speed kills)

• Crowdsourcing equals greater efficacy than silos (collaboration = good)
Antivirus software powerless to stop data breach attacks. CIO.com, 2/9/12

DNSChanger infected half of Fortune 500 in 2012 Computerworld, 2/2/12

Cost of data breaches averages $7.2M, or $214 per customer record per Ponemon Institute, The Atlantic, 2/16/12

...91 percent of cyber attacks begin with a "spear phishing" email... computerworld.co.nz/, Dec 2012

Cyber crime is a permanent part of the Internet tapestry—it’s here to stay
MORE OBLIGATORY DATA POINTS

Top Causes for Security Breaches in 2011

- Malware: 78%
- Phishing: 46%
- OS Vulnerabilities: 31%

Top 3 Types of Threats Posed by Social Media in 2011

- Info gathering attack: 70%
- Malware via compromised sm site: 71%
- Malware via malicious link: 75%

Dealing with rampant malware is time and resource intensive

Source: Information Week
WHAT’S IMPORTANT TO IT SECURITY

The #1 most important metric in determining value of a particular security investment:

- Reduction in incident response time: NO
- Decline in amount of network downtime: NO
- Better risk management strategies: NO
- Decline in breaches: NO
- Better protection of customer records/intellectual property: NO

Fewer man hours spent on security-related issues: YES!
There is no **single** point solution to cybercrime

**Heuristics vs. Signatures** is a false argument
Most orgs don’t have access to *known knowns* and waste cycles determining what’s already been determined.
In 2009, the DHS announced plans to recruit 1,000 cyber professionals over three years. As of 2011, DHS had only managed to hire about 260.

The new model needs to highly leverage human capital.

http://www.cnas.org/csmonitor-cybersecurity-kristin-lord-jacob-stokes
Current silo approaches are costly ...

The lack of shared learning creates efficiency for bad actors

It is truly maddening to see examples of bad guys sharing data, tricks, methods and good guys having no effective way of doing it

Anton Chuvakin, Gartner Research Director
BLACKHOLE EXPLOIT

Black hats are as sophisticated as white hats, sometimes more so…

![Figure 6 Administrator Statistics page](image-url)
The underground ecosystem is well developed and collaborative
Dear Client,

Your parcel has arrived at February 18. Courier was unable to deliver the parcel to you at 18 February 06:33 PM.

To receive your parcel, please, print this receipt and go to the nearest office.

Best Regards, The FedEx Team.

FedEx 1995-2013
From: LinkedIn Notification <innovatorswzz@ataportfoy.com.tr>
Subject: LinkedIn Notification service message
Date: October 11, 2012 6:56:23 AM PDT
To: info@internetidentity.com

LinkedIn
NOTIFICATIONS
Invitation notifications:
   - From Dillon Glover (Your classmate)

PENDING NOTIFICATIONS
   - There are a total of 3 letters awaiting your action. Enter your InBox via this link.

Don’t wish to obtain email info letters? Change your letters settings.

LinkedIn values your privacy. Not once has LinkedIn made your email address open to any other LinkedIn member without your permission. © 2010, LinkedIn Corporation.
Welcome to UPS Team

Dear sales@internetidentity.com,

Dear Client, RECIPIENT'S ADDRESS IS WRONG

Please print out the invoice copy attached and collect the package at our department.

With best regards, UPS Customer Services.

Copyright 2011 United Parcel Service of America, Inc. Your UPS TEAM, the United States Postal Services brandmark, and the color brown are trademarks of United Parcel Service of America, Inc. All rights reserved.

Please do not reply directly to this e-mail. USPS .US will not receive any reply message. For questions or comments, visit Contact UPS.

We understand the importance of privacy to our customers. For more information, please consult the Your UPS .COM Privacy Policy.

This communication contains proprietary information and may be confidential. If you are not the intended recipient, the reading, copying, disclosure or other use of the contents of this e-mail is strictly prohibited and you are instructed to please delete this e-mail immediately.

MyUps_id52....zip (70 KB)
The Threat Economy Is a Thriving Business With Vast Complexity
Negative consequences can be significant...

- Stolen / lost revenue
- Exfiltration of intellectual property
- Erosion of BRAND
- Disruption of network uptime
- Degraded IT reputation
- And the most important loss...

If something happens at your organization, the first question you’ll ask is, “Is it just me or is everybody else getting hit with this attack?” You can’t answer that for yourself…You’ve got to be part of a larger gene pool to get an immediate answer…

— Renee Guttman, Chief Information Security Officer, The Coca Cola Company
Collaboration is critical…

The issue of botnets is larger than any one industry or country. This is why partnership is so important

—Howard Schmidt, former White House Cybersecurity Coordinator

The new model needs to adapt to today’s volume and velocity of information
CONNECT AND COLLABORATE WITH EXISTING TRUST GROUPS

We don’t need another trust group

SCALE your efforts beyond current known contacts - if were hit, chances are you’re not alone

+ Extend your Reach beyond your own island of trust – collaboration can lead to new insights and learnings

+ Leveraging a network to access actionable information faster leads to increased EFFICACY
WHAT WE DO

Information collection, exchange and analytics to produce the best actionable intelligence for the cybersecurity industry

IID’s Threat Data Sources

- Internal Threat Intel Team
- Private Sector
- Gov’t Agencies
- Researchers
- Law Enforcement

ActiveTrust

- Social Collaboration
- Critical Threat Data
- Big Data Enabled Services

Enterprise

Government

ISP’s

OEM
Thank you

Questions?

www.internetidentity.com