When Tinfoil Hats Aren't Enough: Effective Defenses Against APTs

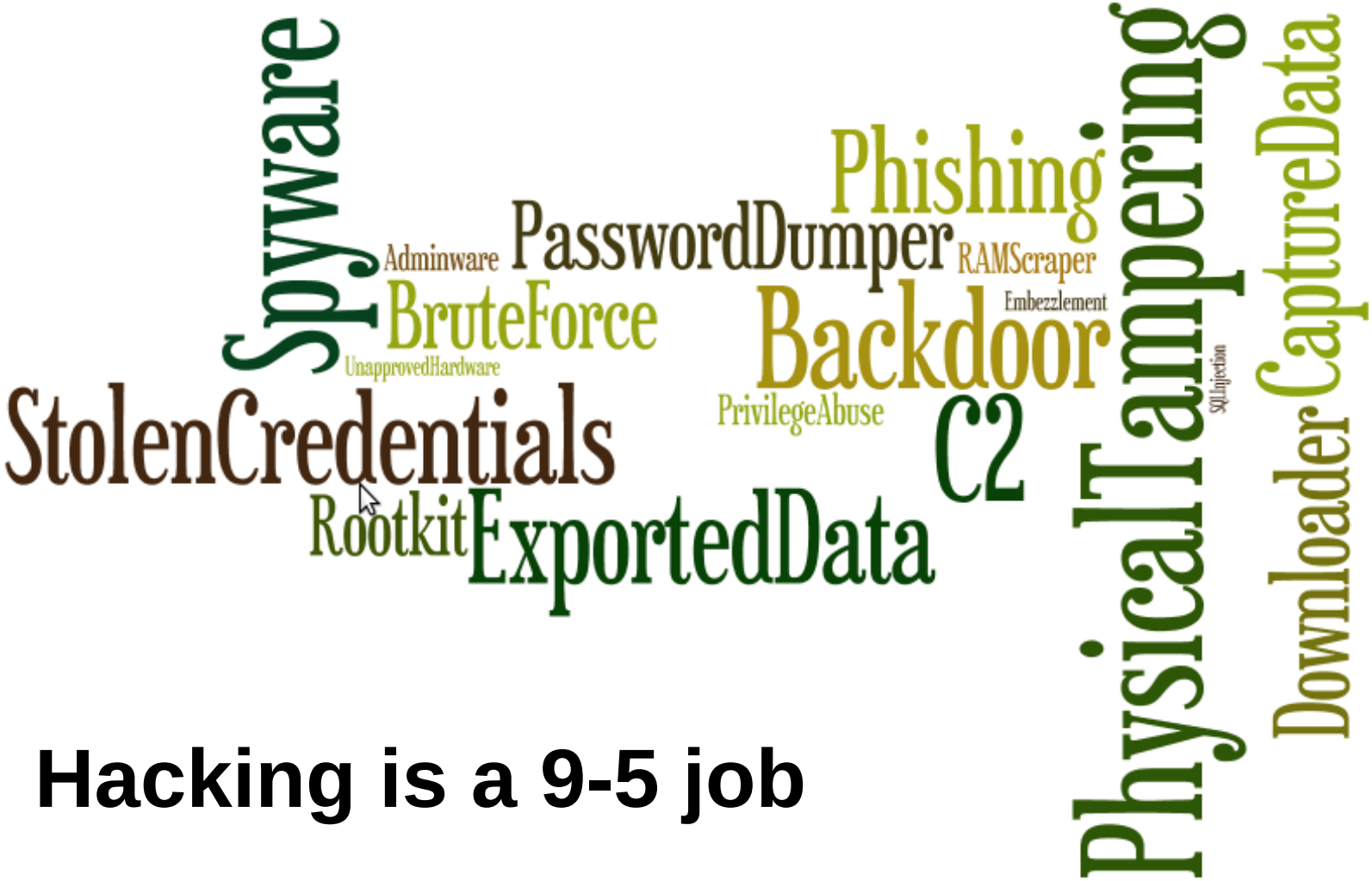
David Corlette, Product Manager

June 11, 2014

NetIQ

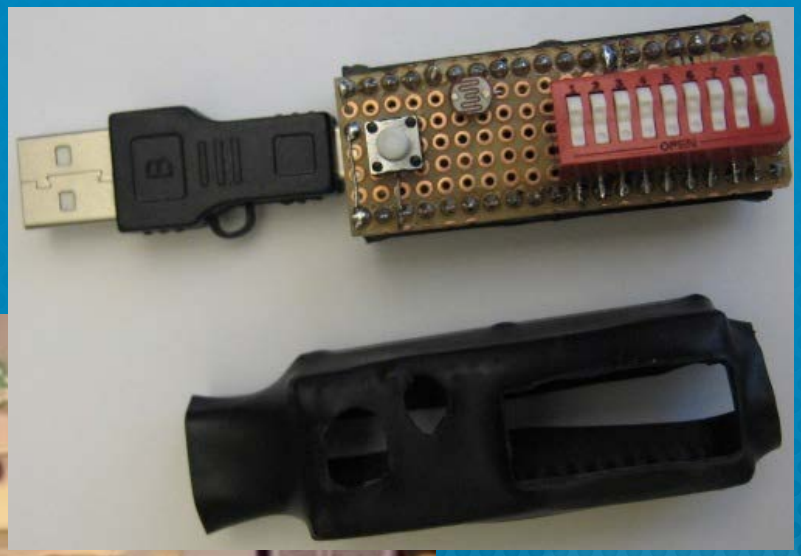
The Problem

Threats are becoming more complex



Hacking is a 9-5 job

USB Programmable Keyboard



Landscape is also more complex

Cloud

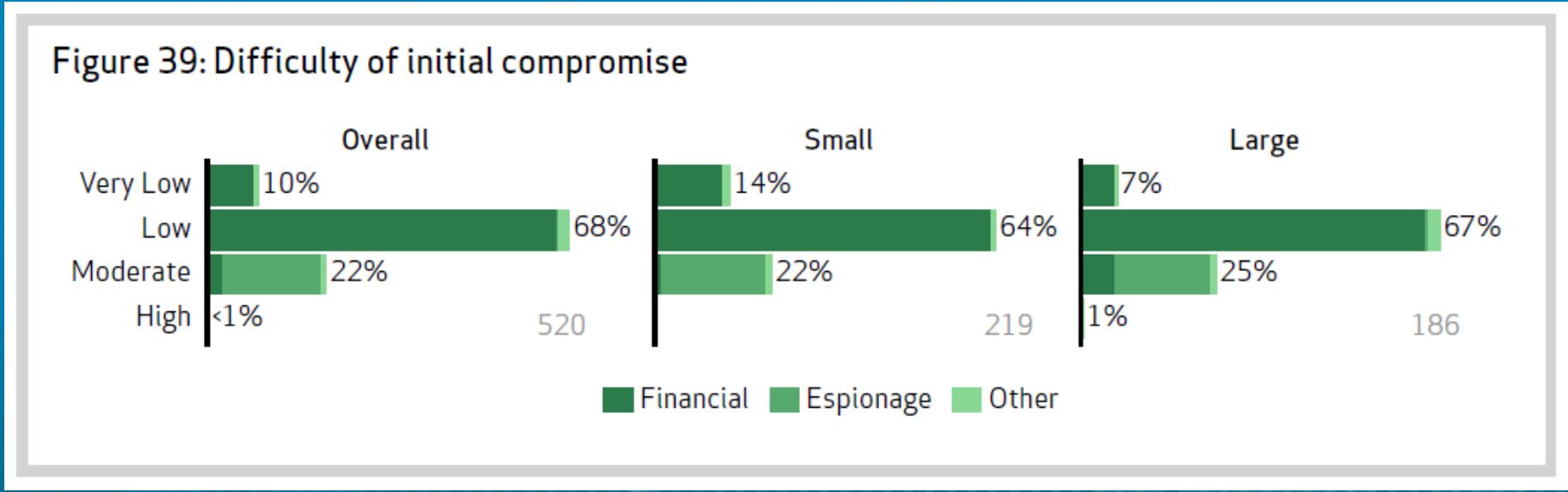
Mobile

BYOD

Social

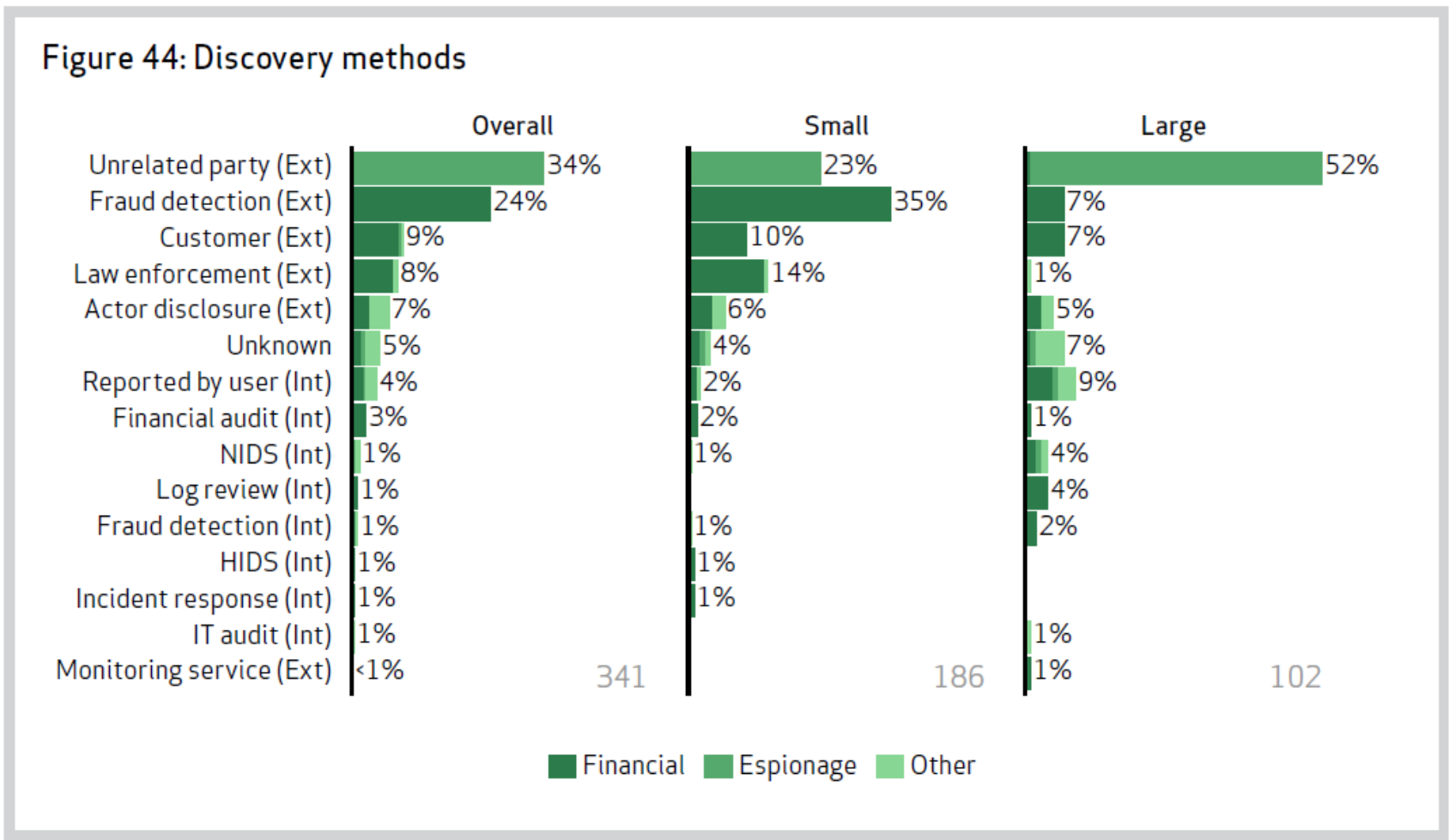
The “attack surface” is ever-expanding

“Not me, we’re safe…”

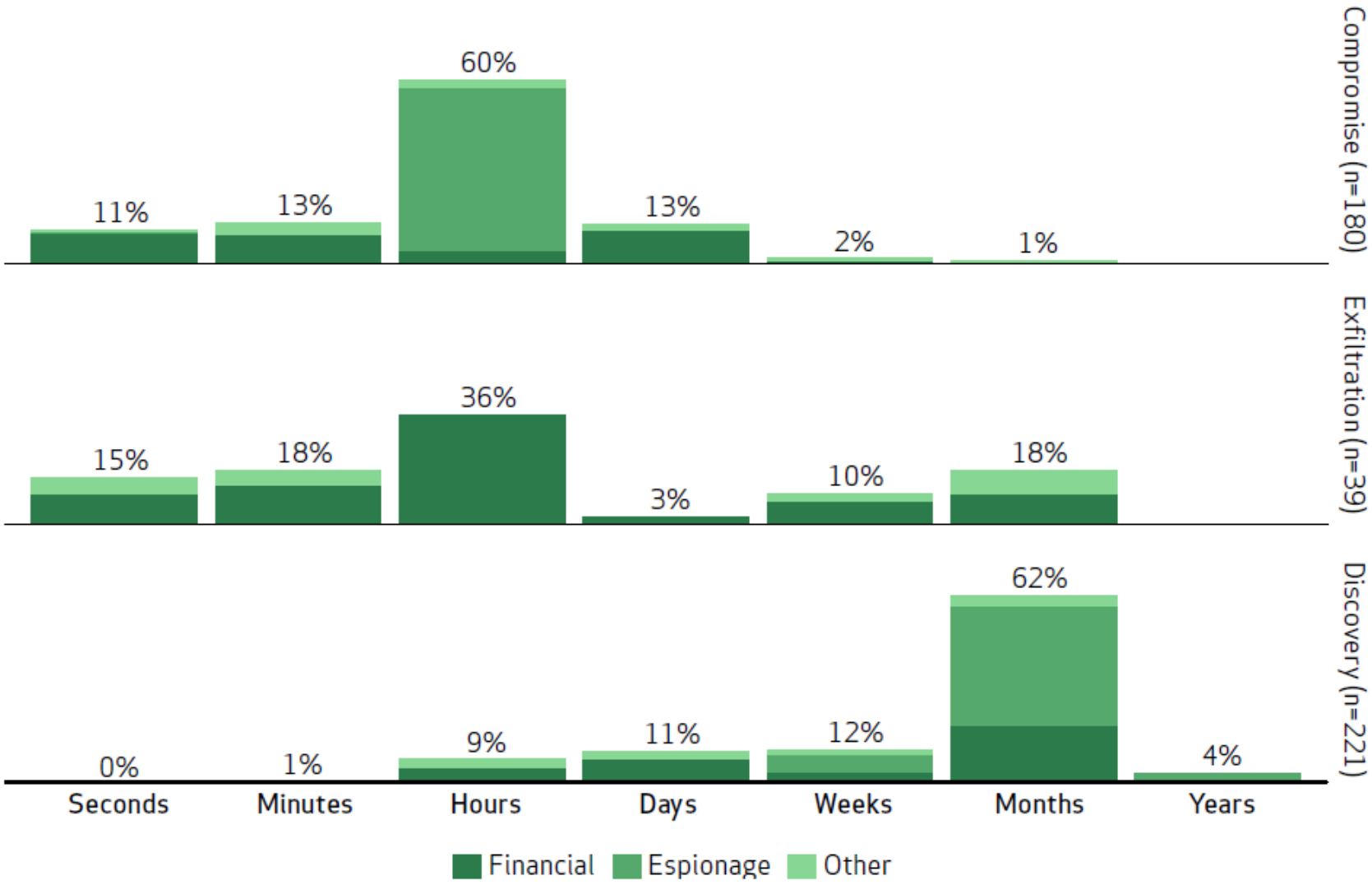


2013 Verizon Data Breach Investigations Report

Insult to Injury



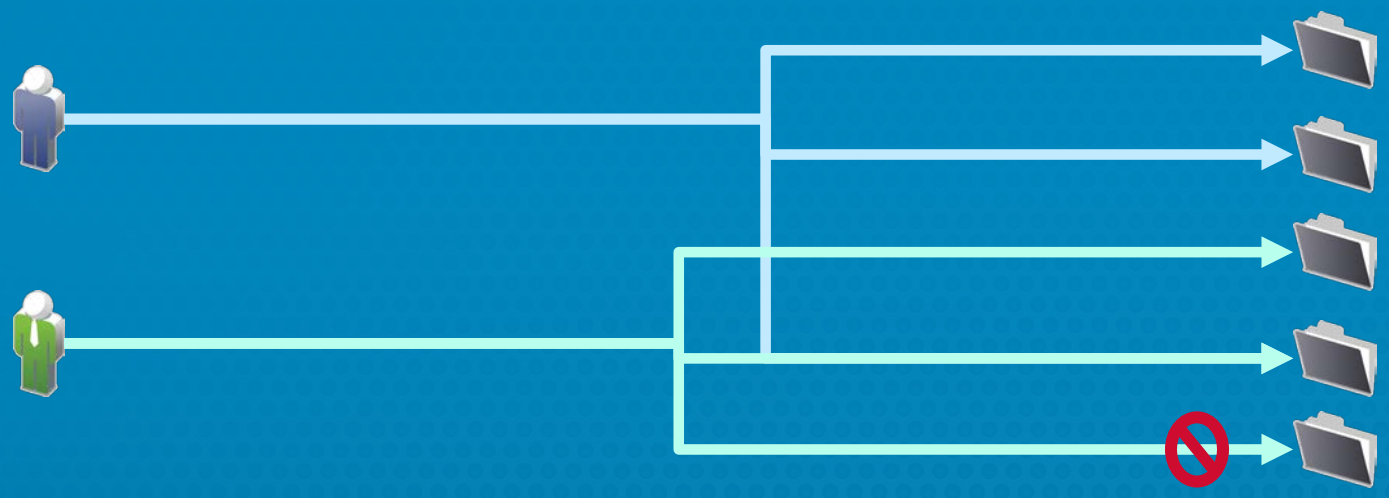
Then Kick You While You're Down



Crusty Shells

Least-privilege Access

$



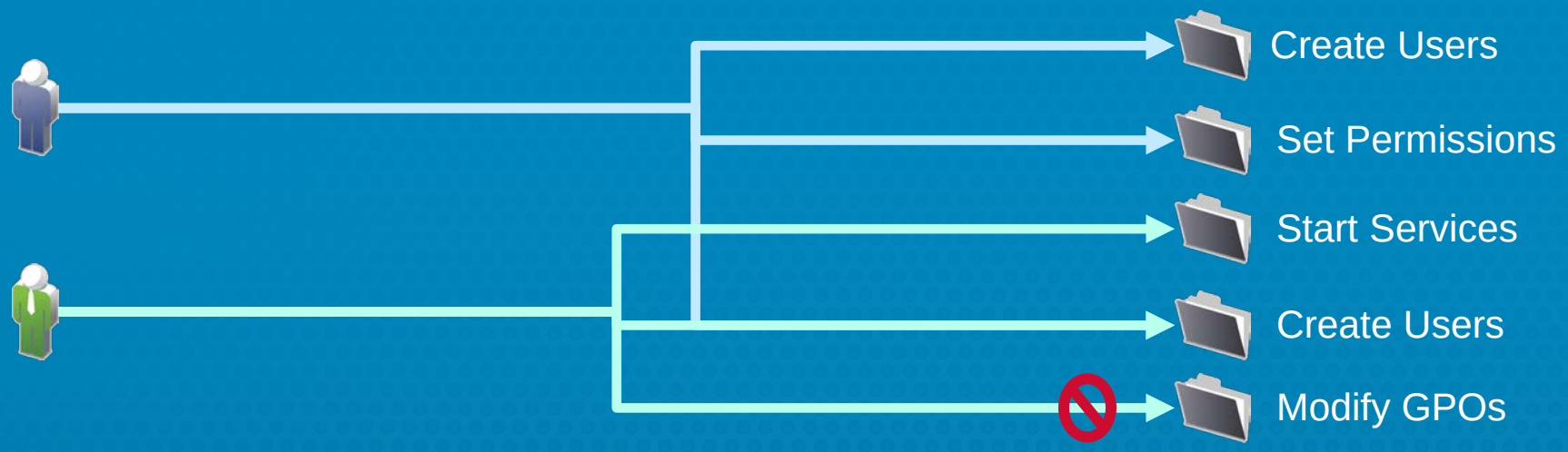
- Role-based access and entitlements
- Request approval workflows
- Automatic real-time de-provisioning

BUT!!!!!!!

- Still have privileged users who can do anything

Privileged User Management

$$



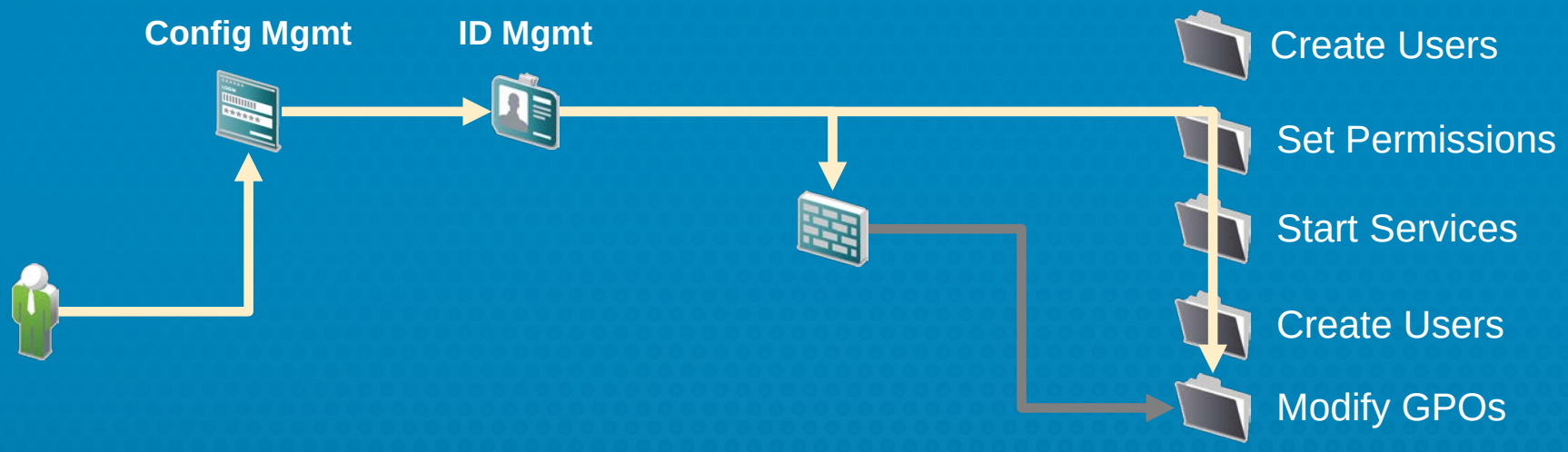
- Granular privileged access and/or password vaults
- Often add finer auditing, keystroke logging

BUT!!!!!!!

- Still have privileged users who can do Bad Things, and you'll only find out afterwards

Dynamic Config Management

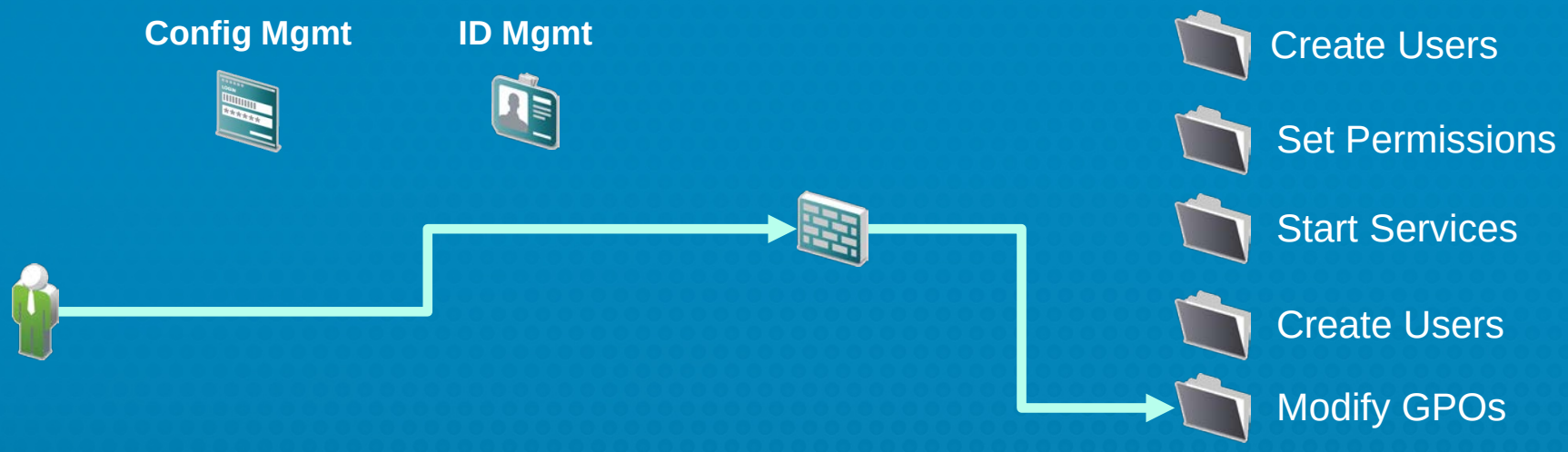
$$$



- Request including what, when
- Approved by N managers/reviewers
- Dynamically provision privileged accounts, secure passwords, even network routes to allow configuration changes to occur

Dynamic Config Management

$$$$



- Monitoring of change to ensure that it adheres to the request parameters
- Auditing, review, and roll-back
- Timeout de-provisioning of access

BUT!!!!!: Still More Issues!

$$$$$

- **Gets really costly**
- Can slow people down
- Still doesn't solve issues of
  - Insider threats (misuse of legitimate access)
  - Malware, stolen credentials
  - Social engineering

So now we need to add:

More Security Products!!

$$$$$

$$$$$

$$$$$

X-Ray Vision

Monitoring vs. Prevention

PREVENTION IS CRUCIAL, AND WE CAN'T LOSE SIGHT OF THAT GOAL. BUT WE MUST ACCEPT THE FACT THAT NO BARRIER IS IMPENETRABLE, AND DETECTION/RESPONSE REPRESENTS AN EXTREMELY CRITICAL LINE OF DEFENSE.

2013 Verizon DBIR

Too much… pressure!

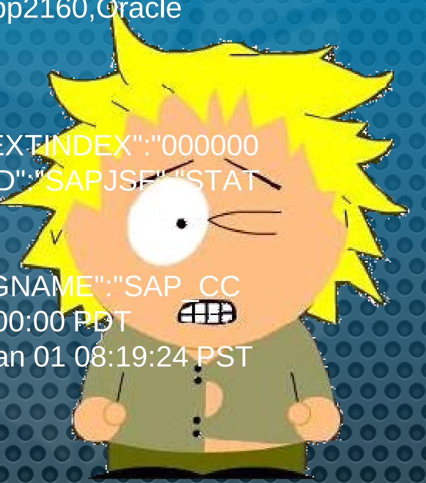
Don Your Eyeglasses

tgMonth="05" tgHour="18" tgDay="13" tgMinute="07" EC="540" C="2" CS="Logon\/Logoff" L="Security" IS="LMURPHY ,TXDOT1 ,(0x15,0xE88A0488) ,3,Kerberos ,Kerberos , ,{cd7b463a-726e-1aec-4fd5-dabe7dc0231e} ,-,- ,- ,- ,- ,144.45.138.69 ,1099" SN="Security" RN="446108" XM="Successful Network Logon: User Name: LMURPHY Domain: TXDOT1 Logon ID: (0x15,0xE88A0488) Logon Type: 3 Logon Process: Kerberos Authentication Package: Kerberos Workstation Name: Logon GUID: {cd7b463a-726e-1aec-4fd5-dabe7dc0231e} Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 144.45.138.69 Source Port: 1099 " tgSecond="12" U="TXDOT1\\LMURPHY" T="Audit Success" ET="4" this="event" CN="HOU-DC" EI="540" tgYear="2010“

1120 0000000000000000002TSV2010-06-02-12.48.43.343776QPADEV000CQSECOFR 600091 QCMD QSYS
*SYSBAS 1 0000000000000000000000000000000000000000QSECOFR OMNIAS2
^@^@^@^@^@^@^@^@^@^@0000001057012915007088230 4AUDRCV0008QSYS *SYSBAS 1 1
^@^@^@^@^@^@^@^B00000000000000000243690
361363360K361362367K365K366367@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

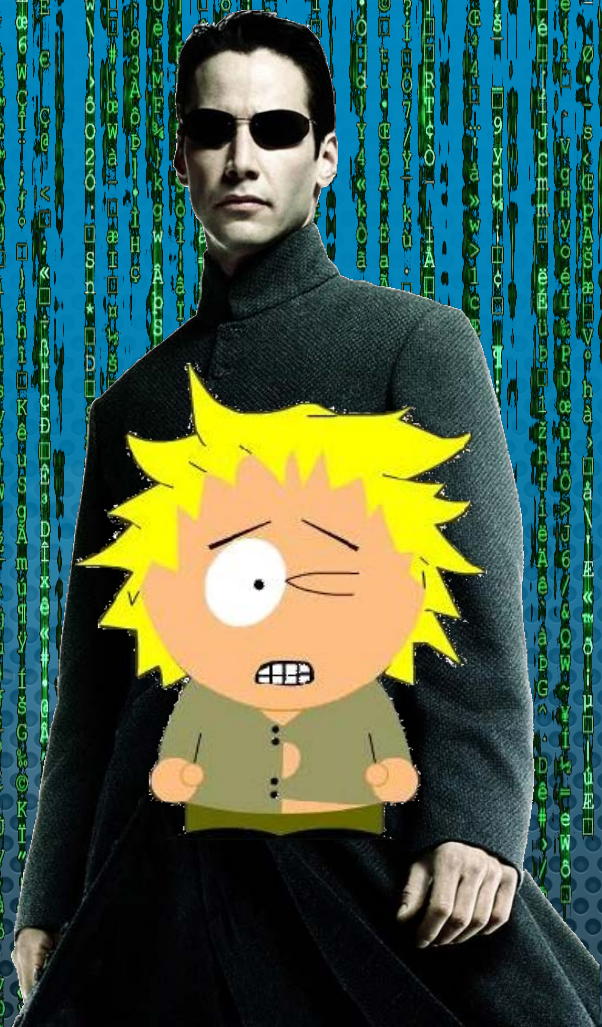
IN090210,ESECDBA,APPLABS\\DLFDTAPP0803,DLFDTAPP0803,2010\/04\/27 18:07:34,2010\/04\/27 18:08:52,2010\/04\/27 18:08:52,101,LOGOFF,,Authenticated by: DATABASE; Client address: (ADDRESS=(PROTOCOL=tcp)(HOST=192.168.170.11)(PORT=2788)),10187,1,1,0,,,,30553,,,,,dlfdtapp2160,Oracle Database 10g Enterprise Edition Release 10.2.0.3.0 – Prod

{"ALERT":{"MANDT":"001","MSG":"Logon Successful (Type=U)","REPORTEDBY":"SecurityAudit","MTMCNAME":"sapserver_DM0_01","ARGTYPE2":"C","EXTINDEX":"0000000012","OBJECTNAME":"Security","MSGARG2":"U&0","MTCLASS":"101","MSGARG1":"AU1","USERID":"SAPJSF","STATUS":"40","ARGTYPE4":"C","STATCHGDAT":"Tue Mar 24 00:00:00 PDT 2009","MTINDEX":"0000000176","VALUE":"2","MSGTEXT":"Security Audit: Logon Event","SEVERITY":"255","STATCHGBY":"SecurityAudit","ALSYSID":"DM0","ARGTYPE3":"C","MSEGNAME":"SAP_CCMS_sapserver_DM0_01","MSCGLID":"AU1","MTNUMRANGE":"033","ALERTDATE":"Tue Mar 24 00:00:00 PDT 2009","FIELDNAME":"Logon","ALUNIQNUM":"0000694352","MTSYSID":"DM0","ALERTTIME":"Thu Jan 01 08:19:24 PST 1970","STATCHGTIM":"Thu Jan 01 08:19:24 PST 1970","RC":"0","MSGID":"AU1","ALINDEX":"0000007340","ARGTYPE1":"C","MSGCLASS":"SAP-YSLOG","MTUID":"0000100010"},"SYSNR":"01","HOST":"192.168.3.7"}



We Can’t All Be Neo

- Who is doing what?
- What access do they have?
- Is that access appropriate?
- Where are they accessing from?
- Is this normal behavior?
- Are there other Indicators of Compromise for the same account/host/service?



A Balanced Plan

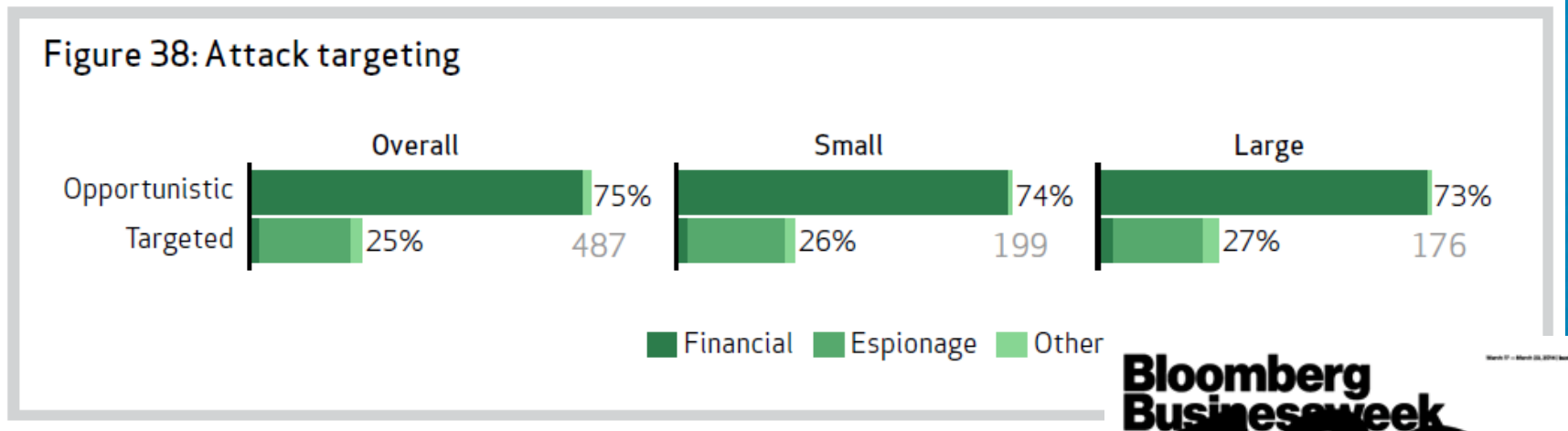
What is the key?

Identity

Remember Poor Tweek

- Who is doing what?
- What access do they have?
- Is that access appropriate?
- Where are they accessing from?
- Is this normal behavior?
- Are there other Indicators of Compromise for the same account/host/service?

Step 1: Don't Be An Opportunistic Target



- Establish a basic level of preventative controls **and monitoring** for all assets
- Make sure all employees know what to watch out for
- Establish basic access controls

Critical Cyber Controls

- Do the easy/cheap ones first!
- Certain initiatives, such as perimeter security and employee training, raise protection level of ALL assets
- Good sources:
  - SANS Top 20: **http://www.sans.org/critical-security-controls**
  - NIST Cyber Security Framework: **http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf**
  - Australian Signals Directorate Top 35 Mitigations: **http://www.asd.gov.au/infosec/top-mitigations/top35mitigations-2014-table.htm**

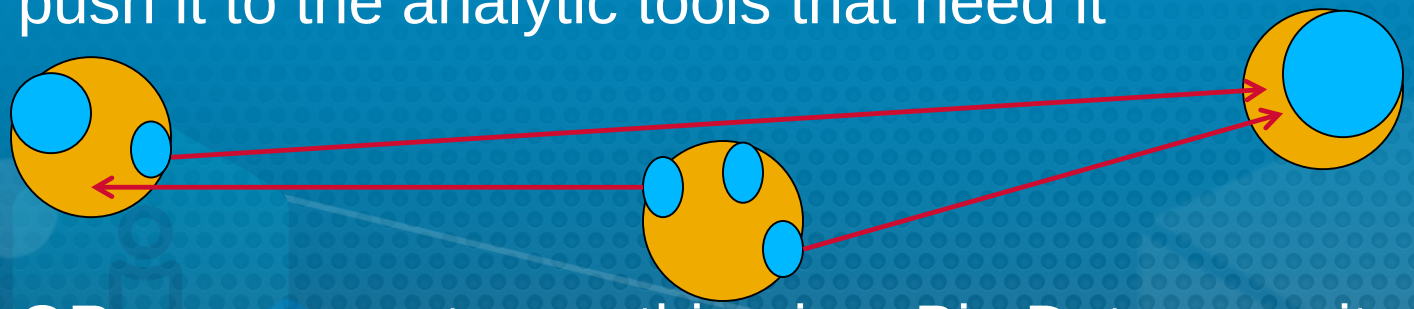
Step 2: Understand Resource Value

Selected Qtr (2015 Q3) Lic/FYM pipeline			
WW/Geo	Late Stage % of Pipeline	Pipeline to Bookings Gap (Ratio)	Total (Qtr) Pipeline
Worldwide	**73.2%**	**6.9**	**$24,527**
North America	73.1%	9.0	$20,273
EMEA	81.2%	4.0	$3,196
APAC	52.6%	2.6	$1,057
Latin America		**0.0**	$0

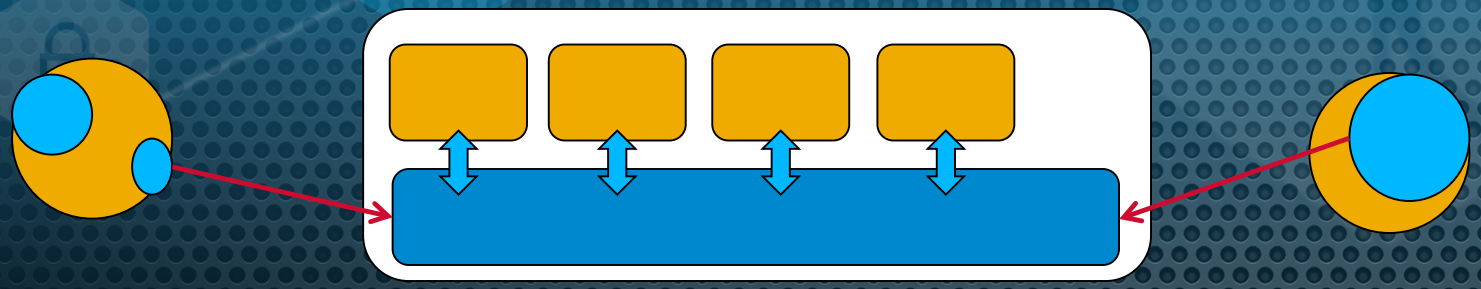
"And then he was like 'whatever' and she said 'no way' and I was like 'ewww…' and she was SO lame that I almost barfed and …"

Where Is My Data?

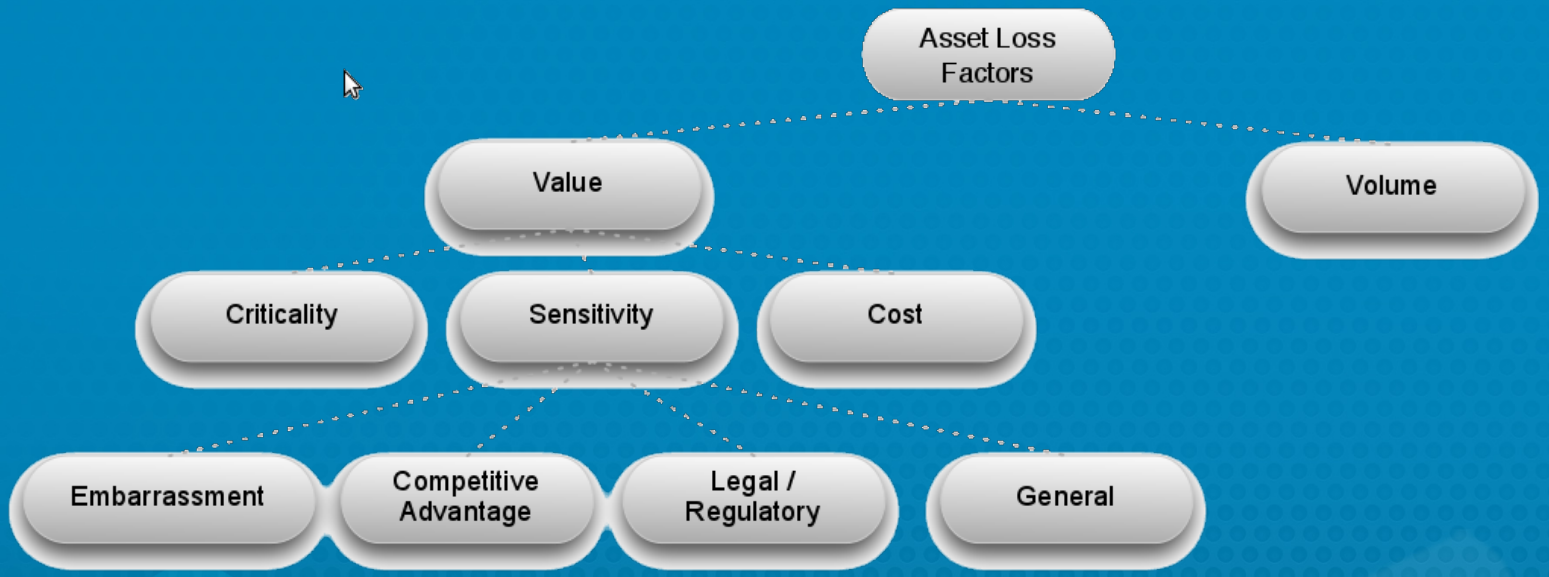
- You probably already have a lot of this information in various forms – CMDBs, directories, agent scan info, server setup logs, etc
- You can extract the data in specific forms and then push it to the analytic tools that need it



- OR you can put everything in a Big Data repository and then bring your analytics to the data



More formally…



Regardless of implementation (Hadoop or Excel) the goals are:

1. Level of investment to protect a given asset should be commensurate with asset value (think of this as **insurance**)
2. Provide inputs to analytics to improve accuracy and prioritization of alerts

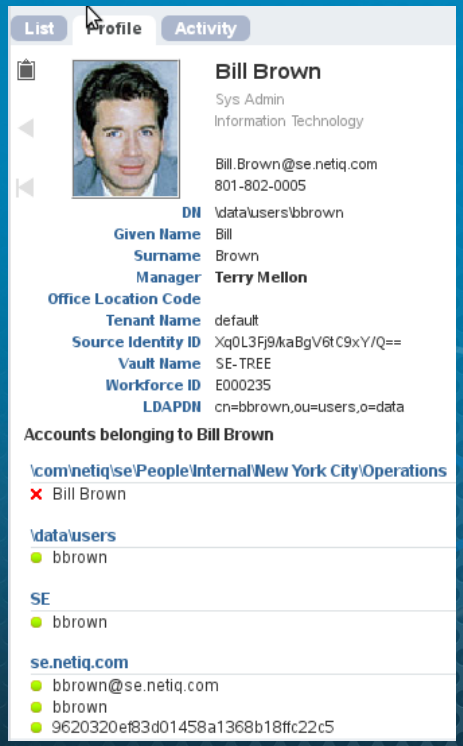
Step 3: Establish Identity Context

- Share Identity context with analytic tools: establish who, what, where
- Start with basic information like contact info, name, location
- Link resources to describe dependencies and relationships: accounts with a person, hosts with a service
- Can extend to things like reputation, sentiment, etc as you get more sophisticated

"On the Internet, nobody knows you're a dog."

Share Identity Context With Monitoring

tgMonth="05" tgHour="11" tgDay="11" tgMinute="42" EC="540" C="2" CS="Logon\/Logoff" L="Security" IS="LMURPHY ,TXDOT1 ,(0x15,0xE88A0488) ,3,Kerberos ,Kerberos , ,{cd7b463a-726e-1aec-4fd5-dabe7dc0231e} ,-,- ,- ,- ,- ,144.45.138.69 ,1099" SN="Security" RN="446108" XM="Successful Network Logon: User Name: BBROWN Domain: TXDOT1 Logon ID: (0x15,0xE88A0488) Logon Type: 3 Logon Process: Kerberos Authentication Package: Kerberos Workstation Name: Logon GUID: {cd7b463a-726e-1aec-4fd5-dabe7dc0231e} Caller User Name: - Caller Domain: - Caller Logon ID: - Caller Process ID: - Transited Services: - Source Network Address: 144.45.138.69 Source Port: 1099 " tgSecond="12" U="TXDOT1\\BBROWN" T="Audit Success" ET="4" this="event" CN="HOU-DC" EI="540" tgYear="2014“



Authentication

March 11, 2014

11:42:12 EST

IP: 144.45.138.69
HN: TXDOT1
DEPT: Finance
Loc: Texas Data Center
Owner: Bill Brown

IP: 144.45.138.69
HN: TXDOT1
DEPT: Finance
Loc: Texas Data Center
Owner: Bill Brown

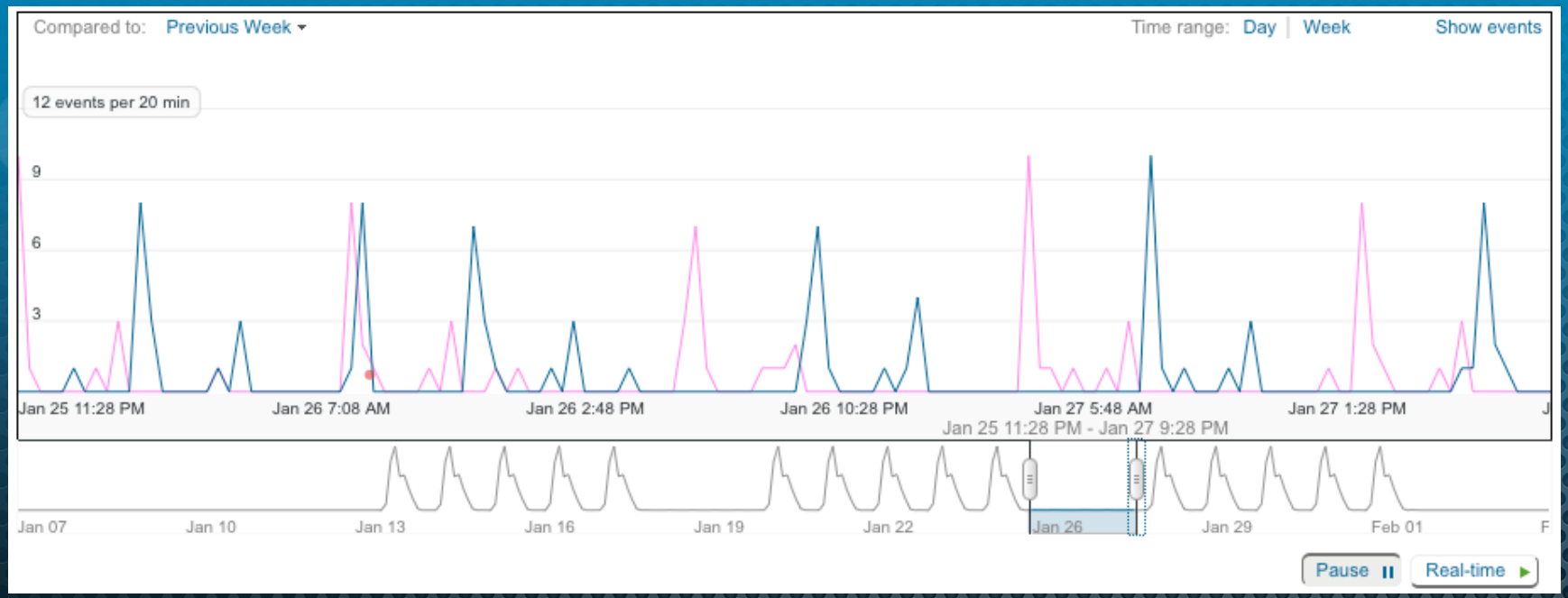
Who

What/When

Where

Step 4: Establish a Baseline

- Understand normal user, host, and service activity
- Leverage this to look for anomalies—changes in behavior
- Use monitoring to compare expected usage against actual usage (e.g. role attestation)



Step 5: Take it To the Next Level

- **WHERE APPROPRIATE,** deploy stronger and more granular access/detection controls to protect your high-value assets
- Take the time to tune and enhance auditing and detection systems – there is no magic bullet as all environments are different

Step 6 to ∞: Keep Improving!

- Invest in technologies, processes, and people to improve detection and research capabilities
- Refine and tune content continuously – analytics, signatures, reports, etc
- Learn from your mistakes!

NetIQ Can Help

Security & Compliance

- Manage and audit user entitlements
- Track privileged user activity
- Protect the integrity of key systems and files
- Monitor access to sensitive information
- Simplify compliance reporting

Identity & Access

- User Provisioning Lifecycle Management
- Centralize Unix account management through Active Directory
- Reduce number of privileged users
- Secure delegated administration
- Windows and Exchange migration

Performance & Availability

- Monitor and manage heterogeneous environments including custom applications
- IT Service validation and end-user performance monitoring
- Dynamic provisioning of large-scale monitoring with exceptions
- Functional and hierarchical incident escalation
- Deliver and manage differentiated service levels

Worldwide Headquarters
1233 West Loop South
Suite 810
Houston, TX 77027 USA

+1 713.548.1700 (Worldwide)
888.323.6768 (Toll-free)
info@netiq.com
NetIQ.com

Join NetIQ's Online QMUNITY

www.netiq.com/communities

© 2014 NetIQ Corporation and its affiliates. All Rights Reserved.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

Copyright © 2014 NetIQ Corporation. All rights reserved.

ActiveAudit, ActiveView, Aegis, AppManager, Change Administrator, Change Guardian, Compliance Suite, the cube logo design, Directory and Resource Administrator, Directory Security Administrator, Domain Migration Administrator, Exchange Administrator, File Security Administrator, Group Policy Administrator, Group Policy Guardian, Group Policy Suite, IntelliPolicy, Knowledge Scripts, NetConnect, NetIQ, the NetIQ logo, PSAudit, PSDetect, PSPasswordManager, PSSecure, Secure Configuration Manager, Security Administration Suite, Security Manager, Server Consolidator, VigilEnt, and Vivinet are trademarks or registered trademarks of NetIQ Corporation or its subsidiaries in the United States and other countries.