RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Will Your Company Be to Intellectual Property What Mt. Gox Was to Bitcoin?

SESSION ID: TRM-W08

Tim Mather

CISO
Cadence Design Systems
@mather_tim

Agenda

- Mt. Gox goes down – similarity to intellectual property loss
- How big is this (intellectual property protection) problem?
- Source of the problem
- Target of the problem
- What to do about ‘internal exfiltration’
- What to do about ‘external exfiltration’
- Summary

Mt. Gox goes down

- “Losses at Mt. Gox have been put at more than $400 million, and experts say it’s not clear whether that money was stolen by criminals or somehow mishandled by the operators of the exchange. Company officials have blamed a glitch in the transaction software that, they say, allowed hackers to siphon away money undetected.”

The Washington Post, 28 February 2014

- 127,000 creditors impacted
- Mt. Gox CEO Mark Karpeles resigned in March, and refused to comply with a court order to testify in person at an April hearing in Washington, D.C. held by the Financial Crimes Enforcement Network, part of the U.S. Department of Treasury

Similarity to intellectual property loss

Avant, Execs Plead No Contest in Code Theft Case

Courts: Software firm agrees to pay $27 million in fines with possibly more to come. Five individuals face jail time.

"Software company Avant Corp., its chief executive and six other current and former executives pleaded no contest Tuesday to criminal charges in the theft of computer code from a rival firm where Avant's founders had worked.

Avant, based in Fremont, Calif., agreed to pay $27 million in fines to Santa Clara County. Avant could be forced to pay Cadence Design Systems Inc. much more in restitution after a hearing next month."

Los Angeles Times, 23 May 2001

- Restitution paid: USD $182 million + interest

cadence™

Not a new problem in Silicon Valley

Two Plead Not Guilty

The New York Times

Published: March 6, 1993

The president and another executive of the Symantec Corporation pleaded not guilty today to charges they stole trade secrets from Borland International, a rival software maker.

Gordon Eubanks, 46, president and chief executive of Symantec, based in Cupertino, Calif., was charged on Thursday with receiving trade secrets from Eugene Wang, 35, a Symantec vice president.

Mr. Wang, hired by Mr. Eubanks from Borland last fall, was accused of stealing confidential information about new software under development by Borland engineers. Both men were charged with conspiring to misuse the information.

If they are convicted, they may face penalties of up to six years in prison and fines of up to $200,000.

Agenda

- *Mt. Gox goes down – similarity to intellectual property loss*
- **How big is this (IP protection) problem?**
- *Source of the problem*
- *Target of the problem*
- *What to do about 'internal exfiltration'*
- *What to do about 'external exfiltration'*
- *Summary*

From an American (only) perspective

"The scale of international theft of **American** intellectual property (IP) is **unprecedented—hundreds of billions of dollars per year**, on the order of the size of U.S. exports to Asia. The effects of this theft are twofold. The first is the tremendous loss of revenue and reward for those who made the inventions or who have purchased licenses to provide goods and services based on them, as well as of the jobs associated with those losses…. The second and even more pernicious effect is that illegal theft of intellectual property is undermining both the means and the incentive for entrepreneurs to innovate, which will slow the development of new inventions and industries..."

[emphasis added]

Source: Report of The Commission on the Theft of American Intellectual Property, dated May 2013

“Chinese military unit charged with cyber-espionage against U.S. firms”

“The [United States] Justice Department on Monday accused five members of the Chinese military of conducting economic cyber-espionage against American companies, marking the first time that the United States has leveled such criminal charges against a foreign country.

Industries targeted by the alleged cyberspying ranged from nuclear to steel to solar energy, officials said. The hacking by a military unit in Shanghai [PLA Unit 61398], they said, was conducted for no other reason than to give a competitive advantage to Chinese companies, including state-owned enterprises.”

Source: *The Washington Post*, 19 May 2014

China says U.S. does the same

China accuses US of hacking country's leaders, businesses and universities

After five Chinese officials were formally charged with hacking by the U.S., China has struck back with accusations of its own.

> *"This behavior is a flagrant violation of international law, a serious human rights violation, threat to the global network security."*
>
> — CHINA INTERNET MEDIA RESEARCH CENTER

The center, affiliated with the Chinese government's State Council, accused the U.S. on May 26 of targeting the country's leaders, scientific institutes, universities, businesses, and cell phone users for digital surveillance. The report summarized documents released by whistleblower Edward Snowden, but did not go into technical detail.

cadence™

#RSAC

RSACONFERENCE2014
ASIA PACIFIC & JAPAN

Some Western media also accuse NSA of same

NSA Laughs at PCs, Prefers Hacking Routers and Switches

BY KIM ZETTER 09.04.13 | 6:30 AM | PERMALINK

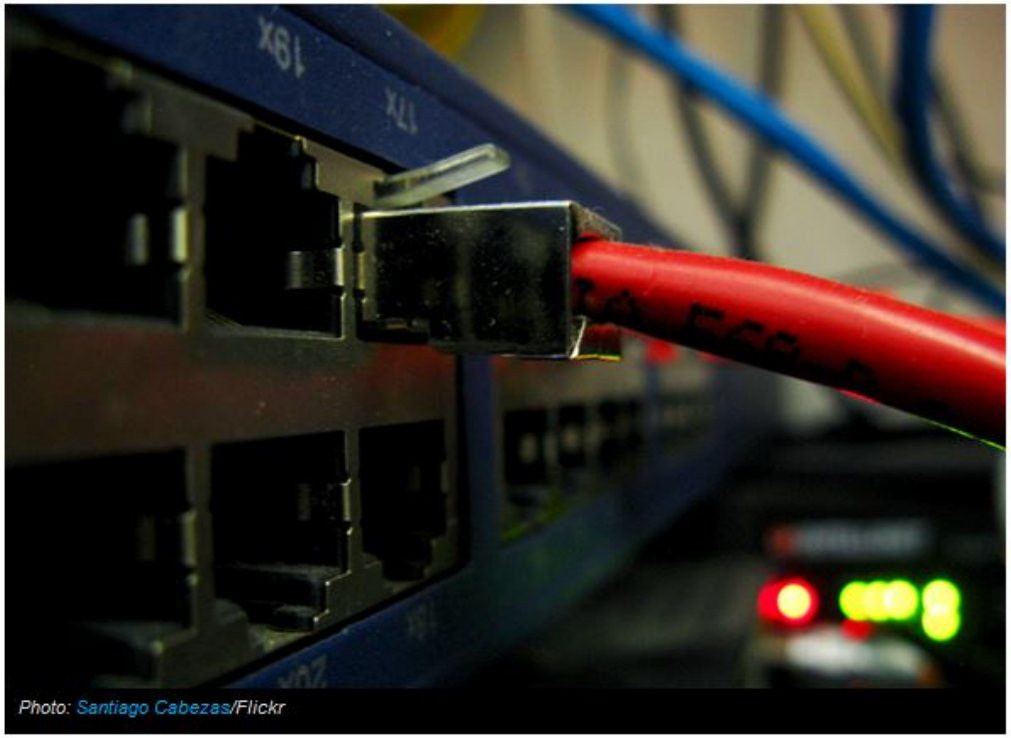


Photo: Santiago Cabezas/Flickr

The NSA runs a massive, full-time hacking operation targeting foreign systems, the latest leaks from Edward Snowden show. But unlike conventional cybercriminals, the agency is less interested in hacking PCs and Macs. Instead, America's spooks have their eyes on the internet routers and switches that form the basic infrastructure of the net, and are largely overlooked as security vulnerabilities.

For information security practitioners, the issue is ***not*** about

cadence™

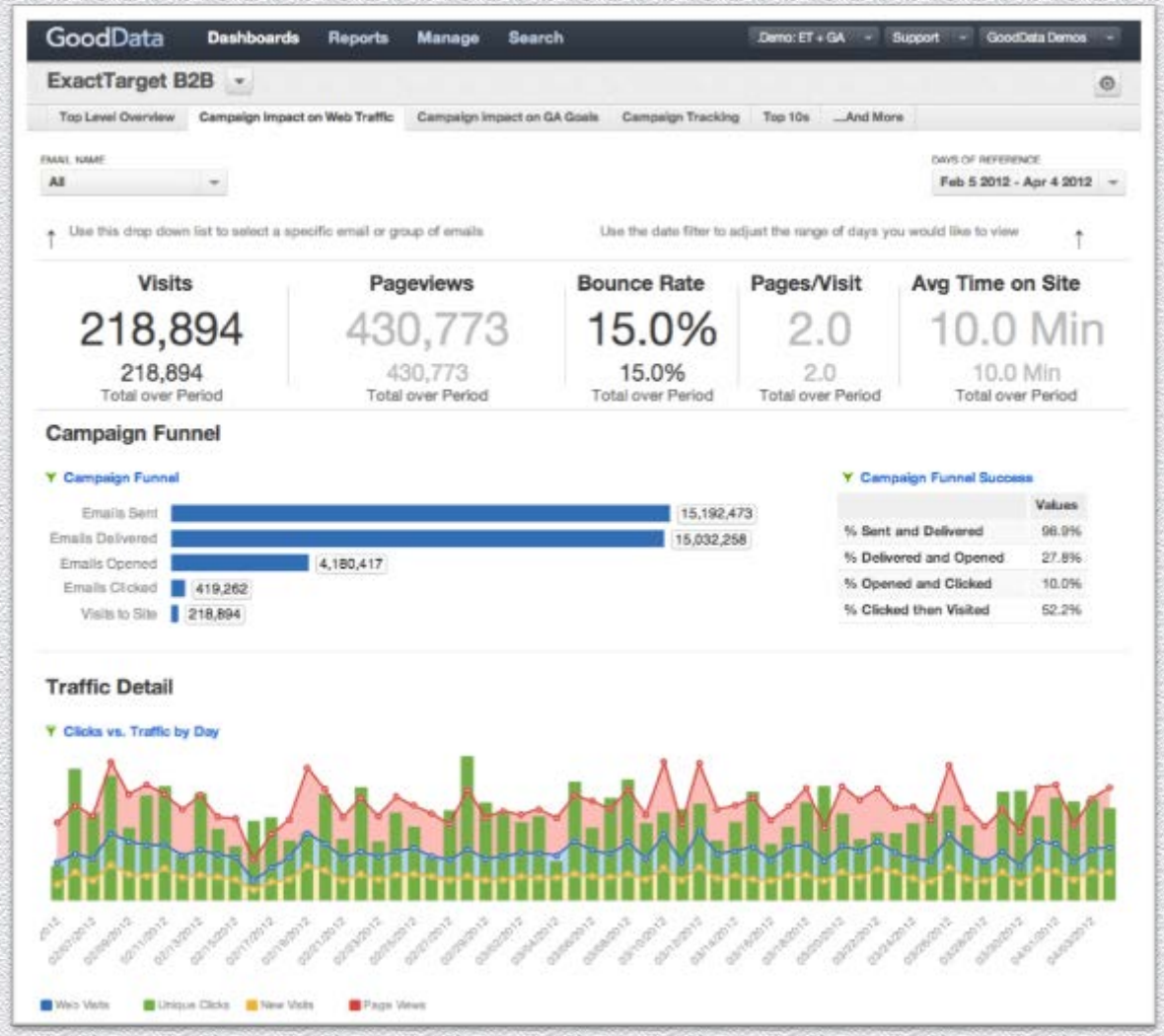
Agenda

- *Mt. Gox goes down – similarity to intellectual property loss*
- *How big is this (intellectual property protection) problem?*
- ***Source of the problem***
- *Target of the problem*
- *What to do about 'internal exfiltration'*
- *What to do about 'external exfiltration'*
- *Summary*

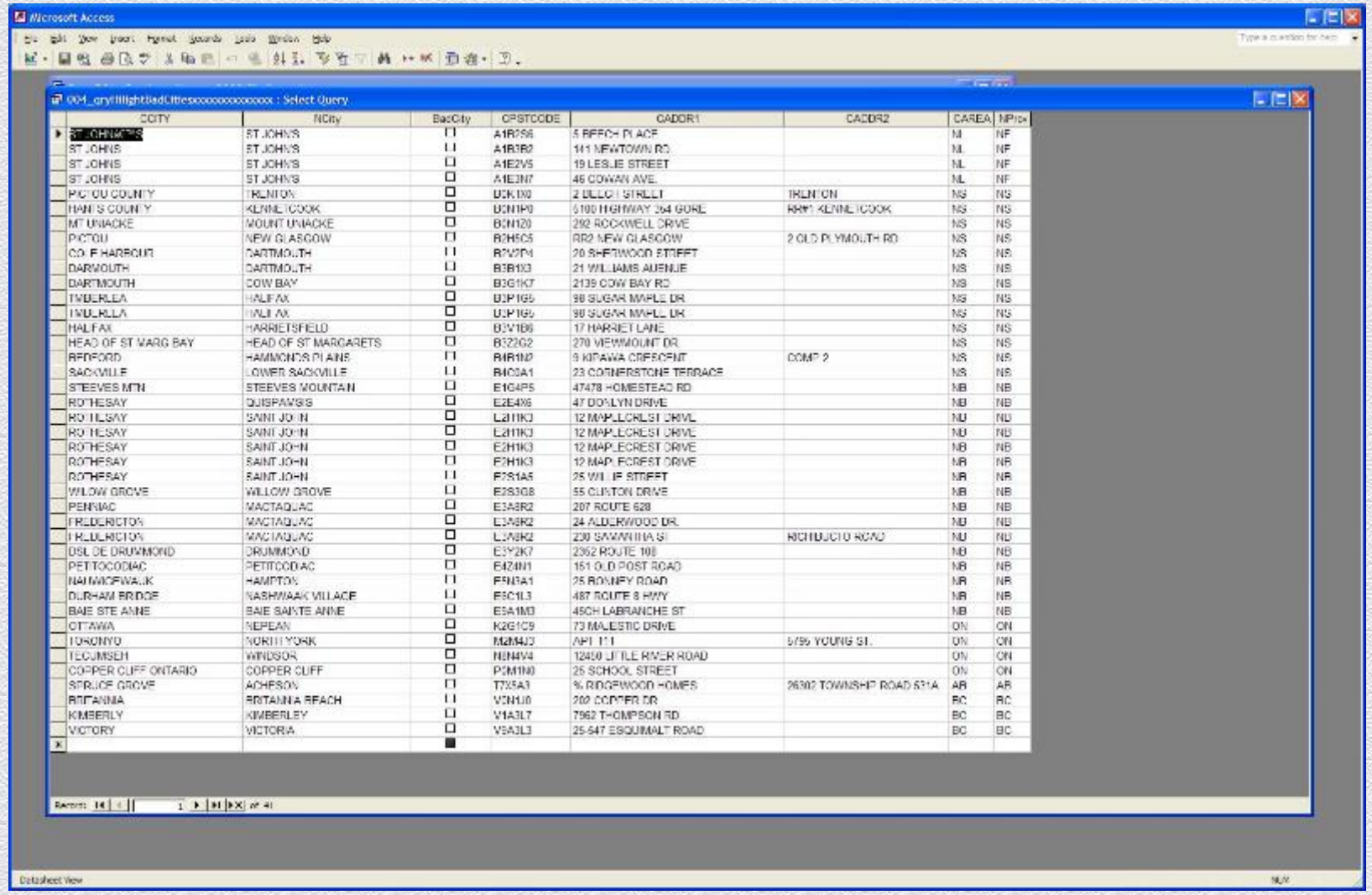
Talented / technical carbon-based life forms – using silicon-based devices

cadence™

Working with semi- and unstructured data



Structured data is less of a problem



CITY	NCity	BadCity	CPSTCODE	CADDR1	CADDR2	CAREA	NPrix
ST JOHN'S	ST JOHN'S	☐	A1B3S6	5 BEECH PLACE		NL	NF
ST JOHNS	ST JOHN'S	☐	A1B3B2	141 NEWTOWN RD		NL	NF
ST JOHNS	ST JOHN'S	☐	A1E2V5	19 LESLIE STREET		NL	NF
ST JOHNS	ST JOHN'S	☐	A1E3N7	46 COWAN AVE		NL	NF
PICTOU COUNTY	TRENTON	☐	B0K1X0	2 DELCO STREET	TRENTON	NS	NS
HANTS COUNTY	KENNETCOOK	☐	B0N1P0	5100 HIGHWAY 354 GORE	RR#1 KENNETCOOK	NS	NS
MT UNIACKE	MOUNT UNIACKE	☐	B0N1Z0	292 ROCKWELL DRIVE		NS	NS
PICTOU	NEW GLASGOW	☐	B2H5C5	RR2 NEW GLASGOW	2 OLD PLYMOUTH RD	NS	NS
CO. H HARBOUR	DARTMOUTH	☐	B2W2P4	20 SHERWOOD STREET		NS	NS
DARMOUTH	DARTMOUTH	☐	B3B1X3	21 WILLIAMS AVENUE		NS	NS
DARTMOUTH	COW BAY	☐	B3G1K7	2139 COW BAY RD		NS	NS
TWEMLEA	HALIFAX	☐	B3P1G5	98 SUGAR MAPLE DR		NS	NS
TWEMLLA	HALIFAX	☐	B3P1G5	98 SUGAR MAPLE DR		NS	NS
HALIFAX	HARRIETSFIELD	☐	B3V1B6	17 HARRIET LANE		NS	NS
HEAD OF ST MARG BAY	HEAD OF ST MARGARETS	☐	B3Z2G2	270 VIEWMOUNT DR		NS	NS
BEDFORD	HAMMONDS PLAINS	☐	B4B1N7	9 KITAWA CRESCENT	COMP 2	NS	NS
SACKVILLE	LOWER SACKVILLE	☐	B4C0A1	23 CORNERSTONE TERRACE		NS	NS
STEEVES MTN	STEEVES MOUNTAIN	☐	E1G4P5	47478 HOMESTEAD RD		NB	NB
ROTHESAY	QUISPAMSIS	☐	E2E4X6	47 DONLYN DRIVE		NB	NB
ROTHESAY	SAINT JOHN	☐	E2H1K3	12 MAPLECREST DRIVE		NB	NB
ROTHESAY	SAINT JOHN	☐	E2H1K3	12 MAPLECREST DRIVE		NB	NB
ROTHESAY	SAINT JOHN	☐	E2H1K3	12 MAPLECREST DRIVE		NB	NB
ROTHESAY	SAINT JOHN	☐	E2H1K3	12 MAPLECREST DRIVE		NB	NB
ROTHESAY	SAINT JOHN	☐	E2S1A5	25 WILLIS STREET		NB	NB
WILOW GROVE	WILLOW GROVE	☐	E2S3G8	55 CURTON DRIVE		NB	NB
PENNIAC	MACTAQUAC	☐	E3A8R2	207 ROUTE 628		NB	NB
FREDERICTON	MACTAQUAC	☐	E3A8R2	24 ALDERWOOD DR.		NB	NB
FREDERICTON	MACTAQUAC	☐	E3A8R2	230 SAWMILL ST	RICHIBUCTO ROAD	NB	NB
DSL DE DRUMMOND	DRUMMOND	☐	E3Y2K7	2362 ROUTE 108		NB	NB
PETTCODIAC	PETITCODIAC	☐	E4Z4N1	151 OLD POST ROAD		NB	NB
NAUWIGEWAUK	HAMPTON	☐	E5N3A1	25 RONNEY ROAD		NB	NB
DURHAM BRIDGE	NASHWAAK VILLAGE	☐	E6C1L3	487 ROUTE 8 HWY		NB	NB
BAIE STE ANNE	BAIE SAINTE ANNE	☐	E9A1M3	45CH LABRANCHE ST		NB	NB
OTTAWA	NEPEAN	☐	K2G1C9	73 MAJESTIC DRIVE		ON	ON
TORONTO	NORTH YORK	☐	M2M4J3	APT 171	5795 YONGE ST.	ON	ON
TECUMSEH	WINDSOR	☐	N8N4W4	12450 LITTLE RIVER ROAD		ON	ON
COPPER CLIFF ONTARIO	COPPER CLIFF	☐	P0M1N0	25 SCHOOL STREET		ON	ON
STRUCF GROVE	ACHESON	☐	T7X5A3	% RIDGEWOOD HOMES	26302 TOWNSHIP ROAD 531A	AB	AB
BRITANNIA	BRITANNIA BEACH	☐	V0N1J0	702 COPPER DR		BC	BC
KIMBERLY	KIMBERLEY	☐	V1A3L7	7962 THOMPSON RD		BC	BC
VICTORY	VICTORIA	☐	V9A3L3	25-647 ESQUIMALT ROAD		BC	BC

What to do about data classification?

- First, it is also a ***business*** problem – not just a (IT) security problem
- Business (non-IT) units are key to understanding and mitigating the problem
- Data classification is key
  - Most important data belongs to (non-IT) business units (BUs)
  - BU responsibility to implement data classification
  - BU knows what data is important to it better than IT – which might not understand the technology or the market for that technology
- Repositories: quite possible that BU does not know about all of 'its' own data repositories, or have control over all of them
  - BU and IT have to work together to establish 'ground truth'

Did I mention **data classification**?

- Or, lack thereof
- How to classify unstructured (and semi-structured) data
  - Accurately
  - Timely – fast
  - Scalably – at scale
- One approach: use meta-data as an indicator of content
- Another approach: content-based categorization
  - Acceptable for storage management
  - Not acceptable for security management
- Another approach: Semantic Web techniques using Resource Description Framework (RDF) or other ontology

Agenda

- *Mt. Gox goes down – similarity to intellectual property loss*
- *How big is this (intellectual property protection) problem?*
- *Source of the problem*
- **Target of the problem**
- *What to do about 'internal exfiltration'*
- *What to do about 'external exfiltration'*
- *Summary*

Internal repositories

Source code:

- ClearCase (IBM) – expensive
- Perforce – widely used

- CVS – open source
- Subversion – open source

- Use of proprietary protocols *might* help discovery
- Use of encrypted network traffic *might* help discovery
- Do not overlook Microsoft Sharepoint – and even
- File servers (yes, you probably still have some of those)

External repositories

Agenda

- *Mt. Gox goes down – similarity to intellectual property loss*
- *How big is this (intellectual property protection) problem?*
- *Source of the problem*
- *Target of the problem*
- **What to do about 'internal exfiltration'**
- *What to do about 'external exfiltration'*
- *Summary*

Getting to ‘ground truth’ – detection

- Multiple tools required for useful / actionable identification; from coarse to more granular:
  - Vulnerability assessment scanners – identification of types of systems
    - For example, Nessus’ Perforce Server Detection plugin
  - IDS / IPS (host- and network-based) – identification of actions
    - Also helpful for traffic analysis
  - DLP (host- and network-based) – identification of content
    - Network-based is needed for TLS and SSH session decryption
  - Correlation across / between these tools (and others) is critical!
    - Use Splunk, or a tool like it (e.g., open source kibana or Sumo Logic)

Proactive action

- Continuous monitoring – previous slide: rinse & repeat
- Blocking unauthorized actions on specific content – DLP
- Restricting unauthorized devices and / or unauthorized actions:
  - USB drives (e.g., Verdasys' Digital Guardian Removable Media Encryption)
  - Wi-Fi (e.g., for Windows OS, per security group via GPO, logon, WMI, or VBS scripts)
  - Bluetooth (e.g., for Windows OS, same as above Wi-Fi)

Reactively: not desired, but can be effective (next time)

- Legal prosecution of offender
- 'Burn' offender to his / her new employer, putting that company on formal, legal notice about stolen IP

cadence™

Agenda

- *Mt. Gox goes down – similarity to intellectual property loss*
- *How big is this (intellectual property protection) problem?*
- *Source of the problem*
- *Target of the problem*
- *What to do about 'internal exfiltration'*
- **What to do about 'external exfiltration'**
- *Summary*

How to find these external repositories?

- Frankly, that is a challenge
- Do you need a specialized cloud discovery service?

- Or, can you find such through traditional on-premise tools using threat intelligence feeds?
  - Egress too (not just ingress): default deny
  - Application (or so-called next generation) firewall required (with TLS and SSH session decryption capabilities)
  - Free and / or vendor agnostic cloud services discovery feed?

No shortage of vendor threat feeds available!

- Arbor Networks
- Cyveillance
- Dell SecureWorks
- HBGeary
- IBM X-Force
- iDefense (VeriSign)
- Intel (McAfee)
- Juniper
- Norse
- Palo Alto Networks
- Secunia
- Symantec
- Trend Micro
- Etc.

cadence™

Lots of free feeds available too

MalwareBlacklist	http://www.malwareblacklist.com/showMDL.php
MalwareDomain List	http://www.malwaredomainlist.com/mdl.php
Malcode	http://malc0de.com/database/
HostFile	http://hosts-file.net/?s=Browse&f=EMD
Dshield	http://www.dshield.org/ipsascii.html
ZeusTracker	https://zeustracker.abuse.ch/monitor.php?browse=binaries
PhishTank	http://www.phishtank.com/
CyberCrime Tracker	http://cybercrime-tracker.net/
MTC SRI	http://mtc.sri.com/live_data/attackers/
Malware Group	http://www.malwaregroup.com/
Cleam MX	http://support.clean-mx.de/clean-mx/viruses
Project Honeypot	https://www.projecthoneypot.org/list_of_ips.php
Iseclab	http://exposure.iseclab.org/about
Palevo Tracker	https://palevotracker.abuse.ch/
Dynamic DNS	http://www.malwaredomains.com/?cat=140
Joe Win Domain Blacklist	http://www.joewein.de/sw/blacklist.htm
Sucuri Labs	http://labs.sucuri.net/
OpenBL	http://www.openbl.org/lists/base.txt
Botscout	http://www.botscout.com/
VX vault	http://vxvault.siri-urz.net/
URLQuery	http://urlquery.net/index.php
JSUnpack	http://jsunpack.jeek.org/dec/go?list=1
Uribl	http://rss.uribl.com/nic/NAUNET_REG_RIPN.xml
Atlas Arbor Networks	http://atlas.arbor.net/summary/fastflux?out=xml
Alienvault	https://reputation.alienvault.com/reputation.data
DYSDYN	http://security-research.dyndns.org/pub/malware-feeds/ponmocup-botnet-domains.txt

Problem though: threat feeds do not track cloud services

- Even ‘cloud proxies’ (e.g., NetSkope, Skyhigh Networks) are not definitive
- Those products have same problem you do: keeping up with storage (and other services) ‘flavor’ *du jour*
- Egress filtering alone is insufficient – too many applications masquerading on HTTP and HTTPS
- Need AppID (Palo Alto Networks) or OpenAppID (Cisco Snort)
- Possible alternative (if already using Splunk): real-time domain look-ups of outlier domains (building your own database of cloud services)

Agenda

- *Mt. Gox goes down – similarity to intellectual property loss*
- *How big is this (intellectual property protection) problem?*
- *Source of the problem*
- *Target of the problem*
- *What to do about 'internal exfiltration'*
- *What to do about 'external exfiltration'*
- **Summary**

cadence™

In sum

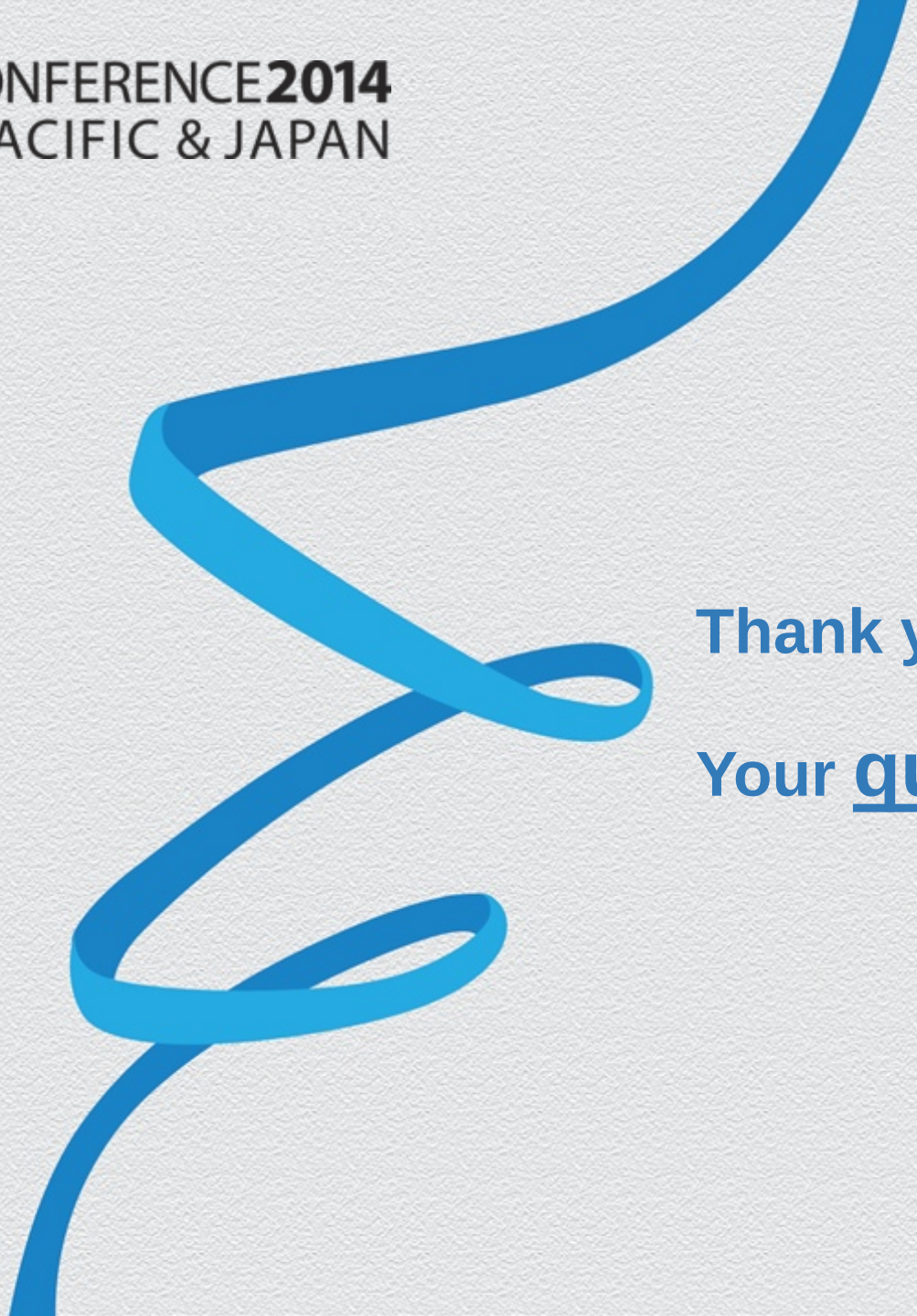
- It all ***starts*** with ***effective*** data classification – if your organization does not have such, then it realistically has nothing in the way of IP protection
- Failure to protect intellectual property (IP) could cost your organization ***significant*** hard and soft dollars – and cost you your job
- Difficult problem! Requires multiple infosec disciplines / skills, multiple infosec tools, and multiple BU cooperation and coordination (e.g., InfoSec, other IT groups, R&D / product units, Legal, HR, and others)
- Must address ***both*** 'internal exfiltration' and 'external exfiltration'

cadence™

Be persistent – this problem / challenge is like

cadence™

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN



Thank you!

Your questions please?