Impact Cyber Trust

Information Marketplace for Policy and Analysis of Cyber-risk & Trust

Driving Trusted Data & Analytics

Homeland Security
Science and Technology

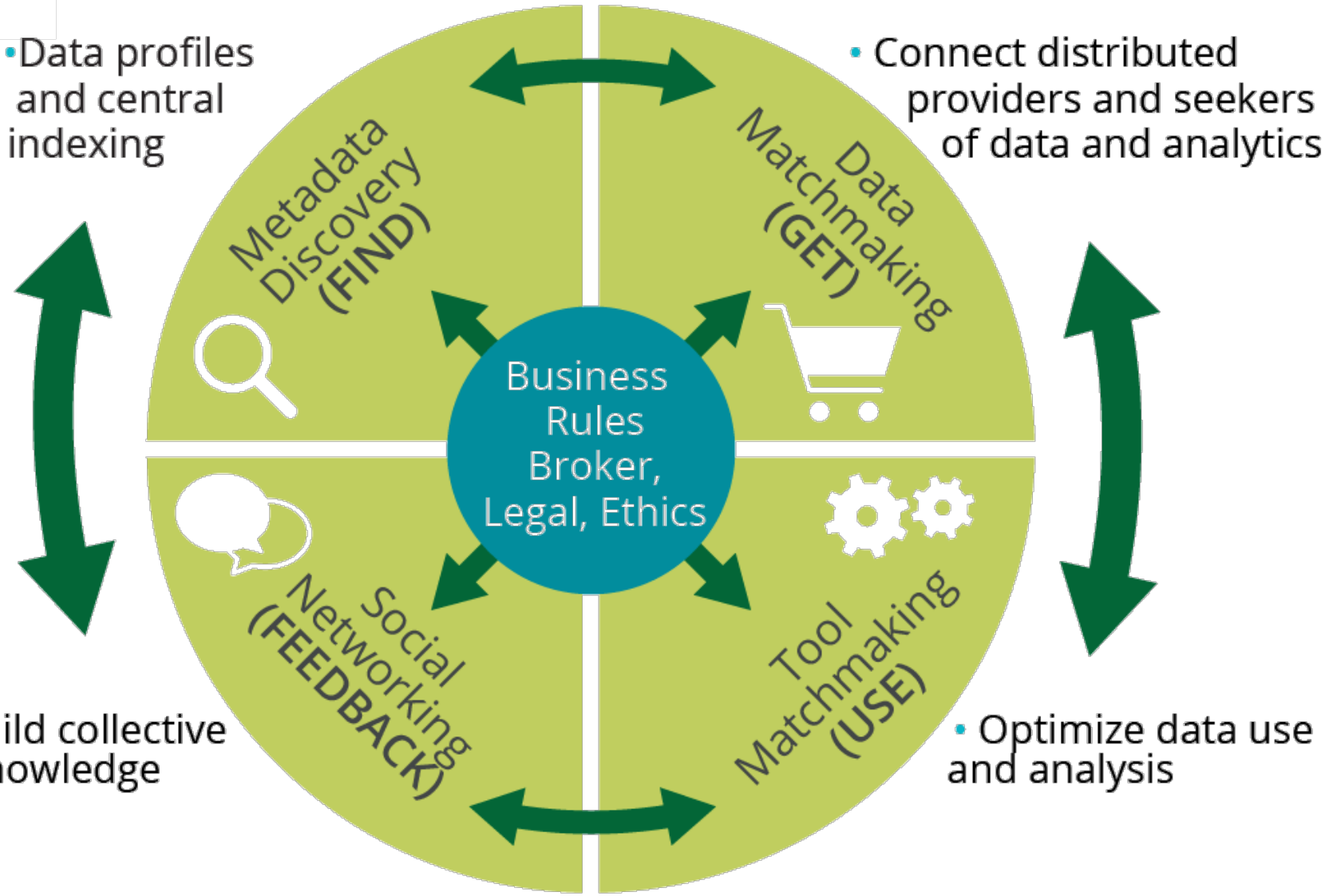
Program Manager:
Erin Kenneally, M.F.S., J.D
Cyber Security Division

IMPACT Motivation: The 'Open Secret' of Effective R&D

- **Data are critical to R&D capabilities**
  - Exactly 0% of R&D (quality) possible sans data
  - Cybersecurity needs real-world data to develop, test, evaluate knowledge & tech solutions to counter cyber threats
  - "Big Data" may grow on trees but still has to be picked, sorted, trucked

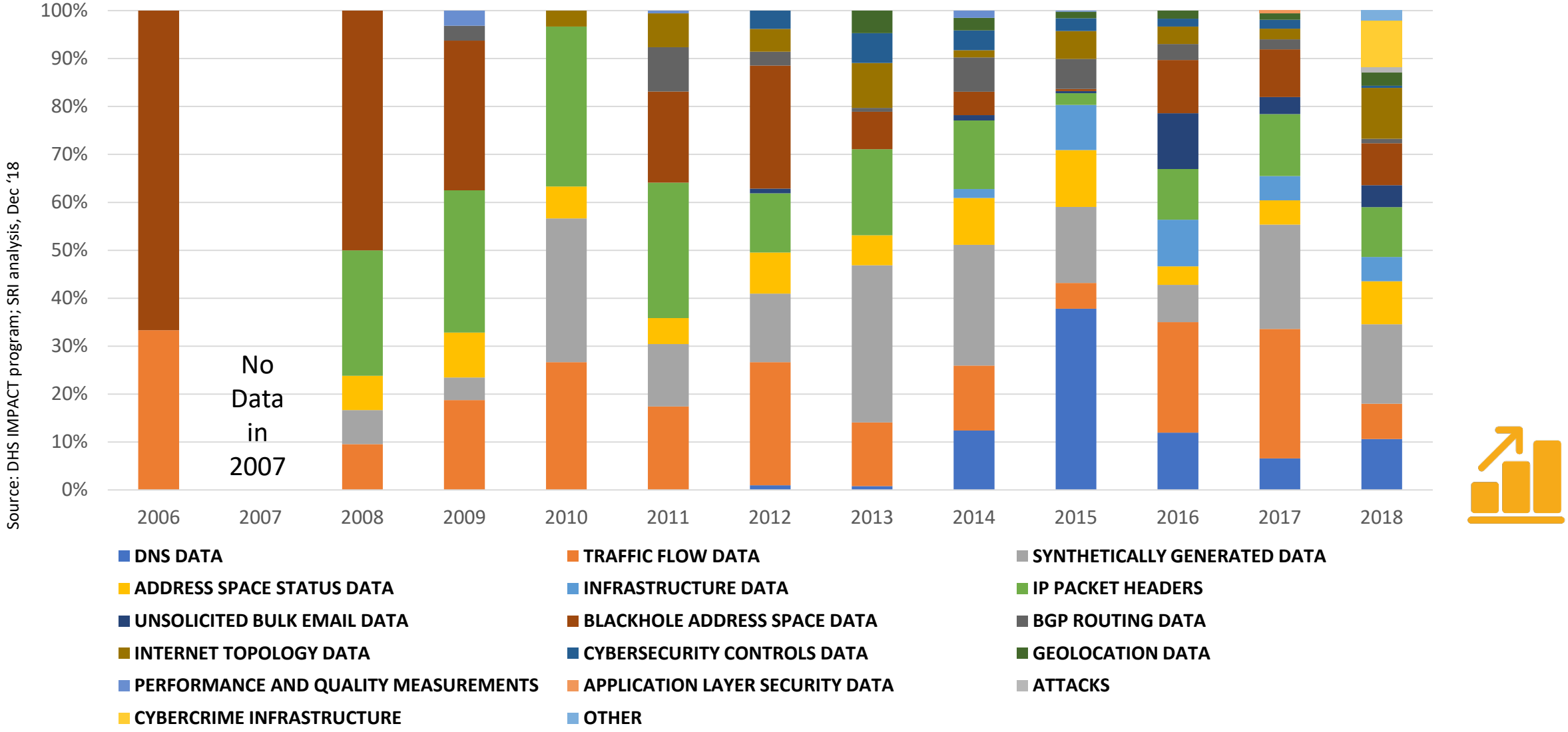
- **Decision analytics are critical to Govt and Industry capabilities**
  - Cybersecurity needs integrated, holistic understanding of risk environment
  - Gap between Data <-->Decisions: multi-dimensional, complex association and fusion, high-context presentation elements

- **Data sharing + Analytics != Easy**
  - High value data = High legal risk + $$
  - Data rich vs. data poor
  - Expensive to abstract away low level knowledge- and labor- intensive tasks
  - Technologists optimize for Efficiency, Lawyers optimize for Certainty



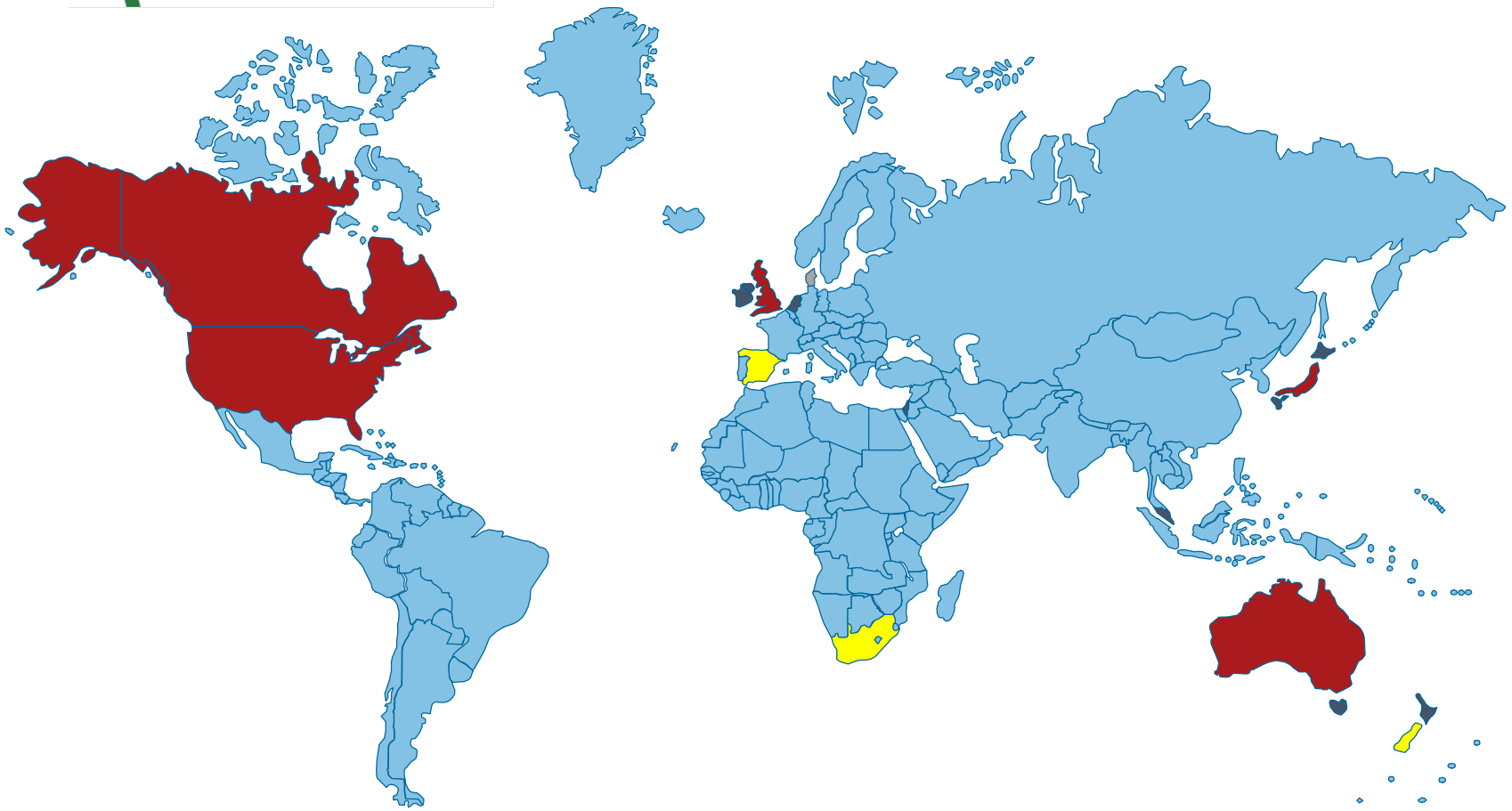
Shop til You Drop IMPACT Portal ImpactCyberTrust.org

Data Trends



Source: DHS IMPACT program; SRI analysis, Dec '18

Customers & Stakeholders



IMPACT customer base encompasses cyber security researchers and developers in 8 partner countries: AUS, CAN, UK, JA, NL, Israel, Singapore

New Zealand, Ireland, Spain, Sweden, Germany, South Africa, Denmark, South Korea all eager to participate. Will onboard under new model pending program's future.

Model- Ahead of its Time

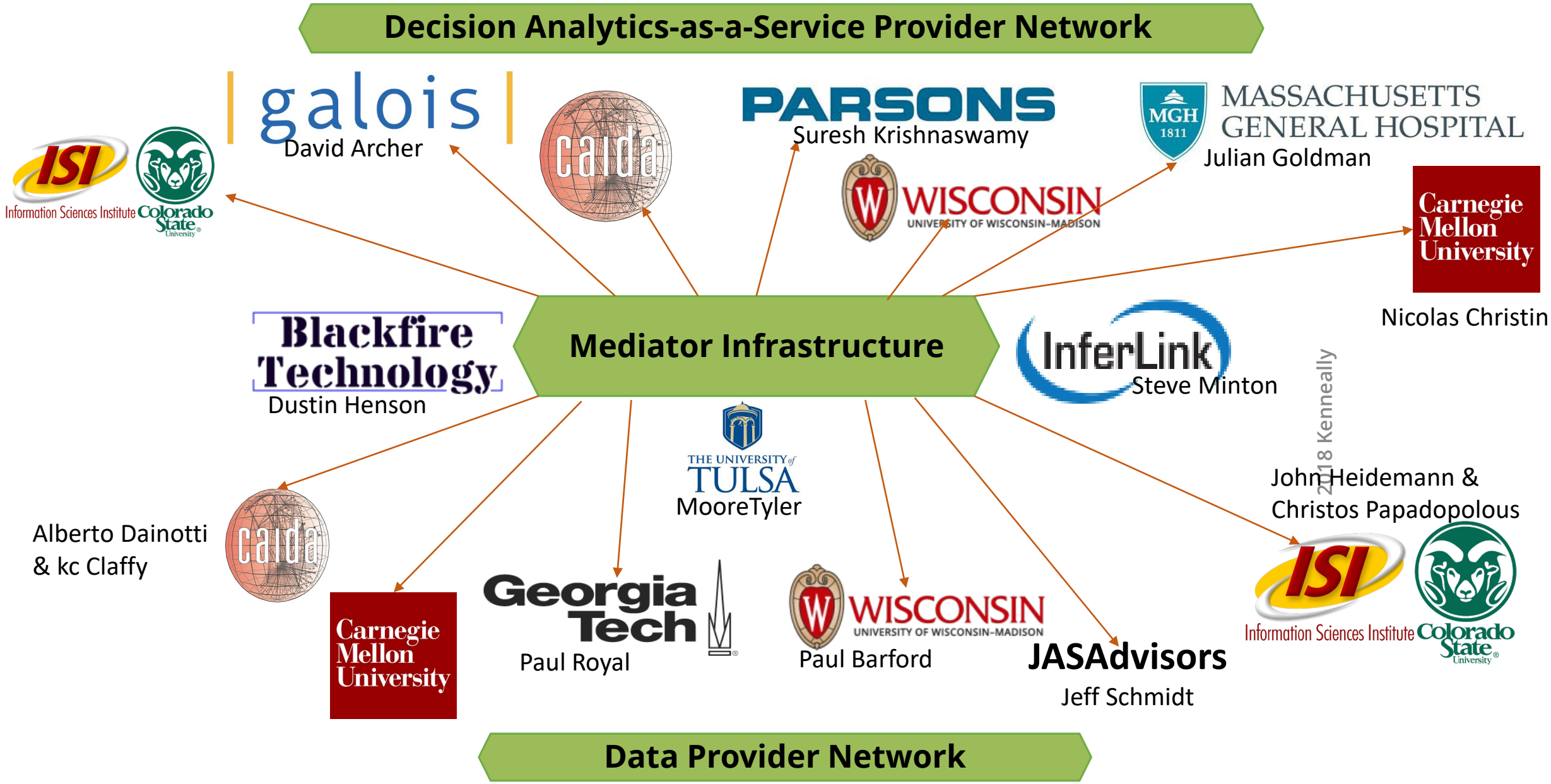
Current method to de-risk data sharing

- Engage in a rigorous internal review of proposed academic research projects.
- Close to half of the companies retain custody and control over the research data at all times.
- Companies employ rigorous data use agreements to limit access to and use of shared data.
- Lots of lawyers
- Easier not to play

How IMPACT addresses risks

- ✓ Vet Researchers, Providers, Data
- ✓ Provider can host and provision own data
- ✓ Provider can engage Disclosure Control-as-a-Service for very sensitive data that allows analysis without Researcher seeing data
- ✓ Provider leverages standardized Researcher data use agreements with customized additional restrictions by Provider

Current Booths in the Marketplace



Data Popularity (2015-18)

Dataset Name	Data Provider
GT Malware Passive DNS Data Daily Feed	Georgia Tech
Historical GT Malware Passive DNS Data 2011-2013	Georgia Tech
US Long-haul Infrastructure Topology	University of Wisconsin
DARPA Scalable Network Monitoring (SNM) Program Traffic	DARPA
Skaion 2006 IARPA Dataset	SKAION
GT Malware Unsolicited Email Daily Feed	Georgia Tech
DSHIELD Logs	University of Wisconsin
syn-flood-attack	Merit Network, Inc.
Netflow-1	Merit Network, Inc.
DoS_traces-20020629	University of Southern California-Information Sciences Institute
NCCDC 2013	Center for Infrastructure Assurance and Security (UTSA/CIAS)
NCCDC 2014	Center for Infrastructure Assurance and Security (UTSA/CIAS)
DoS_80_timeseries-20020629	University of Southern California-Information Sciences Institute
CAIDA DDoS 2007 Attack Dataset	UCSD - Center for Applied Internet Data Analysis
Netflow-2	Merit Network, Inc.
Netflow-3	Merit Network, Inc.
NCCDC 2011	Center for Infrastructure Assurance and Security (UTSA/CIAS)
NTP DDoS 2014	Merit Network, Inc.
NCCDC 2015	Center for Infrastructure Assurance and Security (UTSA/CIAS)
UCSD Real-time Network Telescope Data	UCSD - Center for Applied Internet Data Analysis

Introducing:
The ORDINAL Dataset

Operational Research Data from Internet NAmespace Logs

DNS Namespace Collisions: a (very) quick history

- As old as the DNS itself
- Researched since ~2003
- New interest related to ICANN's new gTLD Program
- Result when resolving party is other than the one anticipated
- "Squatting" and "drop catching" seek to leverage collisions
- Machine-to-machine traffic is more interesting
- Exacerbated by complex/aggressive DNS search path processing
- Misuse of the DNS for Authentication

(known) Violators that Misuse the DNS for Authentication (1)

- Protocols/Applications that lack server authentication
  - Server authentication is hard, think https/tls/x.509, and ssh
  - Especially in scenarios where there is no pre-existing trust
  - Legacy protocols (FTP, POP, etc) mostly punt
- SMTP
  - Identification by DNS MX record; no cryptographic authentication
  - Few use SMTP over TLS to add cryptographic authentication (used for transport)
  - Most email honeypots leverage this behavior

(known) Violators that Misuse the DNS for Authentication (2)

- Microsoft Active Directory, SMB/CIFS
  - Active Directory namespaces are DNS namespaces
  - Locates URL/UNC resources via DNS; trusts the response (!!)
  - \\SYSVOL, \\NETLOGON (!!)
  - \\users\jschmidt and *smb://users/jschmidt*
  - SMB/CIFS will downgrade to WebDAV over http (SharePoint) (!!)
  - Crux of JASBUG/CVE-2015-0008/MS15-011,014
  - Trivially exploitable (Responder and SMBRelay)
  - Microsoft's response, SMB Signing, adds cryptographic authentication
  - "PROPFIND /USERS/michaelw HTTP/1.1" 405 240 "-" "Microsoft-WebDAV-MiniRedir/10.0.10586"
  - "PROPFIND /SYSVOL/XXX/Policies/%7B87DF. . . 48FA9EC%7D HTTP/1.1" 405 293 "-" "Microsoft-WebDAV-MiniRedir/6.1.7601"

(known) Violators that Misuse the DNS for Authentication (3)

- Microsoft Distributed File System (DFS)
  - DFS Namespaces are DNS Namespaces
  - "PROPFIND /DFSRoot02/05_0139/10_General/30_Communication/02_Management_People/info%20in%20verband%20met%20nieuwe%20CAT%20systeem%20in%20EMS HTTP/1.1" 405 338 "-" "Microsoft-WebDAV-MiniRedir/6.1.7601"
- WPAD
  - http://wpad.microsoft.com/wpad.dat (and iterations/subdomains)
  - No authentication; very bad; trivially exploitable (Responder has a module)
  - "GET /wpad.dat HTTP/1.1" 404 206 "-" "WinHttp-Autoproxy-Service/5.1"

(known) Violators that Misuse the DNS for Authentication (4)

- Microsoft System Center Configuration Manager (SCCM)
  - Formerly Systems Management Server (SMS); widely deployed
  - Uses http and custom method: CCM_POST
  - No discernable server authentication
  - "CCM_POST /ccm_system/request HTTP/1.1" 501 214 "-" "ccmhttp”
  - "GET /SMS_MP/.sms_aut?SITESIGNCERT HTTP/1.1" 404 213 "-" "SMS CCM 5.0”
  - "HEAD /SMS_DP_SMSPKG$/4885f087-977b-4a79-b1b6-e4370a25492c HTTP/1.1" 404 - "-" "SMS CCM 5.0"
- Microsoft “OutlookAnywhere”
  - Uses http and custom methods: RPC_IN_DATA, RPC_OUT_DATA
  - "RPC_IN_DATA /rpc/rpcproxy.dll?d89b673c-38b0-483c-b906-89e992c88c12@XXX.com:6001 HTTP/1.1" 501 215 "-" "MSRPC”
  - "RPC_OUT_DATA /rpc/rpcproxy.dll?d89b673c-38b0-483c-b906-89e992c88c12@XXX.com:6001 HTTP/1.1" 501 216 "-" "MSRPC”
  - No discernable server authentication

(known) Violators that Misuse the DNS for Authentication (5)

- Other/Custom Applications
  - "GET /system/transSession.asp?loginusername=KylieXXX&ucomp=01&sysname=E-Freight%20Payment%20System HTTP/1.1" 404 221 "http://epayment.XXX.corp.com/system/login.aspx" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/45.0.2454.101 Safari/537.36”
  - "GET /sm_login/sm_login.asp?user-id=phemingXXX&password=<muchsadness>&ismd5=1&app-id=cmwin.19.45.1602.0&timeout=30 HTTP/1.1" 404 219 "-" "-”

(known) Violators that Misuse the DNS for Authentication (6)

- Just plain Evil
  - "PROPFIND /SysVol/XXX.corp.com/scripts/IR/IRD/ChangePassword.vbs HTTP/1.1" 405 275 "-" "Microsoft-WebDAV-MiniRedir/6.1.7600”
  - "PROPFIND /it/Installs/Work%20Station/Standard%20Applications/GPINSTALL/Local%20Admin%20Password%20Change HTTP/1.1" 405 310 "-”
  - "PROPFIND /home/deebXXX/passwords/keepass HTTP/1.1" 405 257 "-”
  - "GET /Citrix/XenApp/site/changepassword.aspx HTTP/1.1" 404 236 "-" "Mozilla/5.0 (iPhone; CPU iPhone OS 7_0 like Mac OS X)
  - “PROPFIND /Wallpaper/SCREENSAVER.jpg HTTP/1.1 "-”

What is in the ORDINAL Dataset

- CORP.COM
- 02PROXY.COM
- ANAMS1.COM
- ANAMS2.COM
- ANAMS3.COM
- ANAMS4.COM
- ANAMS5.COM
- ANAMS6.COM
- DEFAULT-FIRST-SITE-NAME.COM
- IISPROXY.COM
- LVFS1-2K.COM
- OAUTHPROXY.COM
- SIPEXTERNAL.NET
- SIPINTERNAL.NET
- VLAN01.COM
- VLAN101.COM
- VLAN141.COM
- VLAN142.COM
- VLAN143.COM
- VLAN144.COM
- VLAN145.COM
- VLAN400.COM
- VLAN403.COM
- VLAN404.COM
- VLANB.COM
- WNADROOT.COM

(And There's More!)

DNS Search Path ala Microsoft

“Devolution is a Windows DNS client feature. Devolution is the process by which Windows DNS clients resolve DNS queries for single-label unqualified hostnames. Queries are constructed by appending PDS to the hostname. The query is retried by systematically removing the left-most label in the PDS until the hostname + remaining PDS resolves or only two labels remain in the stripped PDS. For example, Windows clients looking for "Single-label" in the western.corp.contoso.co.us domain will progressively query Single-label.western.corp.contoso.co.us, Single-label.corp.contoso.co.us, Single-label.contoso.co.us, and then Single-label.co.us until it finds a system that resolves. This process is referred to as devolution.”

- Microsoft

(https://technet.microsoft.com/library/security/971888)

Why some names (corp.com) are special

- Microsoft long ago suggested folks name Active Directories “CORP”
- AD hosts and resources have DNS records : <stuff>.corp
- SRV qnames we see at corp.com (among millions of others):
  - _kerberos._tcp.dc._msdcs.Fareast.Microsoft.corp.com
  - _kerberos._tcp.dc._msdcs.redmond.microsoft.corp.com
  - _kerberos._tcp.NA-WA-EXCH._sites.dc._msdcs.Fareast.Microsoft.corp.com
  - _kerberos._tcp.NA-WA-RED._sites.dc._msdcs.redmond.microsoft.corp.com
  - _ldap._tcp.dc._msdcs.middleeast.microsoft.corp.com
  - _ldap._tcp.dc._msdcs.redmond.microsoft.corp.com
  - _ldap._tcp.microsoft.corp.com
  - _ldap._tcp.NA-WA-RED._sites.microsoft.corp.com

More qnames we actually see at corp.com
(just for fun)

wpad.partners.microsoft.corp.com

wpad.redmond.microsoft.corp.com

xboxcontroltower.microsoft.corp.com

isatap.redmond.microsoft.corp.com

itgproxy.northamerica.microsoft.corp.com

itgproxy.redmond.microsoft.corp.com

LUCIS-CXXX.redmond.microsoft.corp.com

UnifiedSearchCube.partners.microsoft.corp.com

Data we collect

- Currently available in ORDINAL:
  - Anonymized DNS querylogs (named logs)
- Collected and may be made available on a case-by-case basis:
  - Email metadata (verbose Postfix logs)
  - Email delivered to the domain (maildir/ format)
  - Port 80 and 443 requests (httpd log)
  - pcaps
- IPv4 and IPv6 served here
- Open to running experiments (based on risk assessment)

A few stats… one month in 2018

Unique v4 IP addresses sending DNS queries to corp.com authoritative DNS nameservers	**182,612** (Mainly from large recursives)
Unique v4 IP addresses requesting WPAD configurations from the HTTP server hosted at corp.com	**379,403** (IPs of specific end machines received over HTTP)
Unique v4 IP addresses requesting information from the HTTP/WebDAV server hosted at corp.com related to NETLOGON or SYSVOL – the most dangerous items as described in MS15- 011/014	**75,272** (IPs of specific end machines received over HTTP)
Unique v4 IP addresses requesting information from the HTTP/WebDAV server hosted at corp.com related to USERS – home directory file system mounts	**27,051** (IPs of specific end machines received over HTTP)
Unique v4 IP addresses sending ns1.labs.jasadvisors.com unsolicited DNS UPDATE queries	**140,643** (Mainly IPs specific Microsoft Active Directory Member Machines taken off-site)

ORDINAL Day In The Life (2018-01-10)

- count(*) where sld = 'corp.com’: 2,877,118
- count(distinct (qname,clientip)) where sld = 'corp.com’: 1,206,480
- Top 5 clients by query count:
  - 203.167.x.x 19,126
  - 213.170.x.x 14,513
  - 67.216.x.x 13,119
  - 41.169.x.x 10,657
  - 213.170.x.x 10,576

Takeaway: Not isolated to a few misconfigured clients

ORDINAL Day In The Life (2018-01-10)

- All 5 RIRs are represented:
  - apnic, arin, ripencc, afrinic, lacnic
- Top 5 netblocks:
  - 74.125.0.0/16 254,069
  - 69.240.0.0/12 209,777
  - **2001:1890::/29 166,144 ← We see quite a bit of IPv6**
  - 76.96.0.0/11 110,891
  - 173.194.0.0/16 82,381

Takeaway: Not isolated to a few (English-speaking) geographies

ORDINAL Day In The Life (2018-01-10)

- Top 5 qnames into corp.com:
  - wpad.corp.com — 83,607 ← Known vulnerable
  - corp.com — 76,109 ← Active Directory related (rr=SRV)
  - srv.corp.com — 70,160 ← Active Directory related
  - null.corp.com — 23,742 ← ?
  - _ldap._tcp.dc._msdcs.corp.com — 18,226 ← Active Directory related
  - msoid.corp.com — 11,152 ← Active Directory related
  - _kerberos._tcp.dc._msdcs.corp.com — 11,033 ← Active Directory related

Takeaway: Mostly related to Microsoft technologies

ORDINAL Day In The Life (2018-01-10)

- count(distinct (qname,clientip)) where qname like '%wpad%’: 28,488
- count(distinct (qname,asn)) where qname like '%wpad%’: 2,383
- count(distinct (qname,netblock)) where qname like '%wpad%’: 5,058
- count(distinct (qname,netblock)) where qname like '%apple%’: 315
- count(distinct qname) where qname like '%microsoft%’: 28 ☺
- count(distinct qname) where qname like '%china%’: 19

Thank You!

For More Information:

IMPACT Program

http:// ImpactCyberTrust.org

Program Manager:

Erin Kenneally, M.F.S., J.D.

DHS Cyber Security Division

ORDINAL Dataset

Search in IMPACT Portal

http://ordinal.jasadvisors.com

jschmidt@jasadvisors.com