Analyze.
Validate.
Remediate.

Manage Risk Not Spreadsheets.

Understanding the Ins and Outs of Cyber Security Risk:

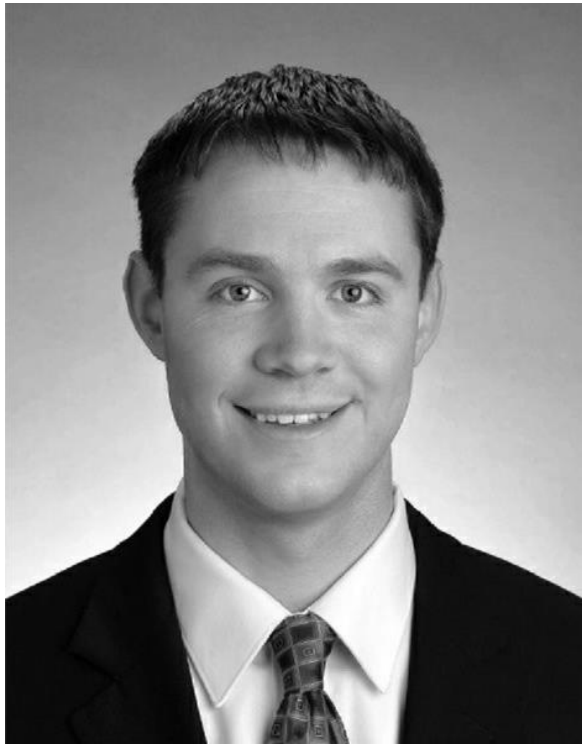
Learning From an External View

CYBERCLARITY360
A DUFF & PHELPS PRODUCT

Introductions

Imran Jaswal
Managing Director,
CyberClarity360

Kevin Braine
Managing Director and Head of EMEA
Kroll Compliance Risk and Diligence



Ryan Spelman
Senior Manager
CyberClarity360

Webinar Overview

- The value objective “Outside-In” data can bring to your third-party cyber risk management program:
  - Importance of Cyber Risk during Due Diligence
  - What is “Outside-In” data?
  - “Outside-In” data within our CyberClarity360 third-party cyber risk assessment platform
  - How other parts of Kroll are using it for clients

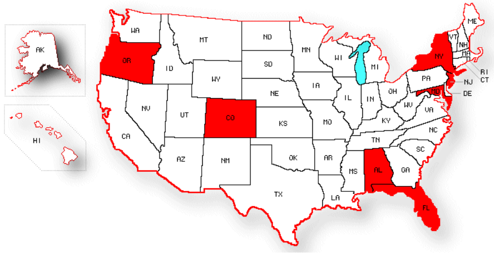
Why is Cyber Risk Important During Due Diligence?

Organizations Hold Valuable Information Wanted by Cyber Attackers

- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Bank & Credit Card Accounts
- IP & Trade Secrets
- Sensitive Business Intelligence

Increasing Regulations…

State



- Alabama
- New Jersey
- Maryland
- New York (DFS/SHIELD)
- Nevada
- Florida
- Colorado
- Oregon
- …

Supply Chain

CMMC/DFARS

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Data Privacy

GDPR

CALIFORNIA
CONSUMER
PRIVACY ACT

HIPAA
Health Insurance Portability & Accountability Act

Potential for Significant Financial Losses

2019: Global average cost of a data breach = $3.92 million.[1]

Extortion Attempts

Business Interruption

Reputational Damage

Loss of customer and supplier trust

Regulatory Action

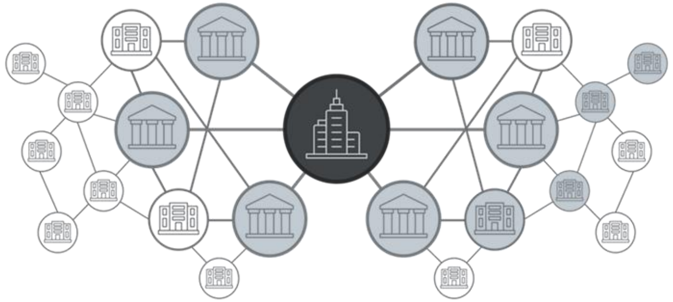
Negligence & Breach of Contract Claims

[1] Ponemon Institute

Typical Cyber Risk Mitigation Use Cases

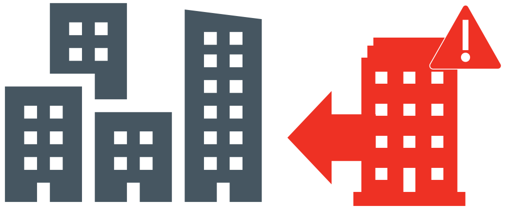
Mergers & Acquisitions

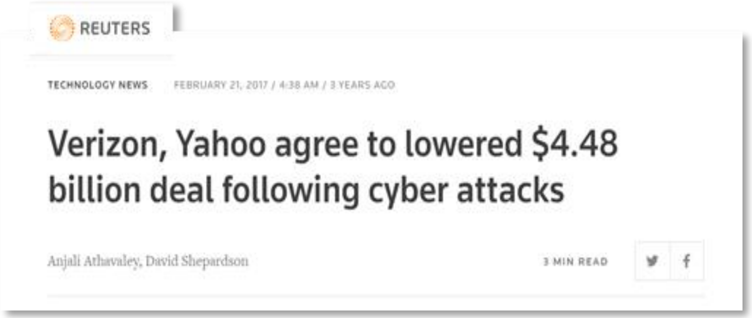
Supply Chain



Mergers & Acquisitions

“Am I buying a breach?”





REUTERS

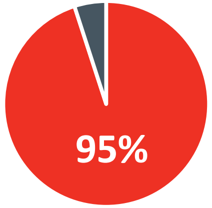
TECHNOLOGY NEWS FEBRUARY 21, 2017 / 4:38 AM / 3 YEARS AGO

Verizon, Yahoo agree to lowered $4.48 billion deal following cyber attacks

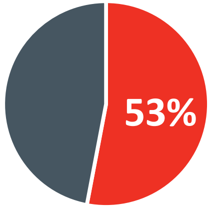
Anjali Athavaley, David Shepardson

3 MIN READ

Drivers



M&A professionals considered cybersecurity a tangible asset



Critical cybersecurity issues or incidents jeopardized M&A deals

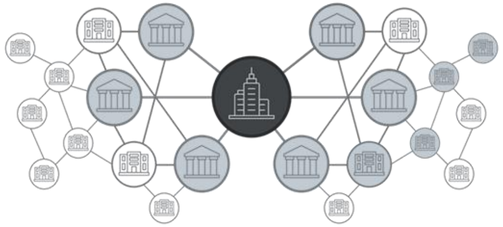
When?

- Before selection
- Post-closing

Supply Chain

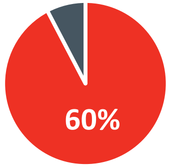
Many 3rd parties have technology integrated into client products or have access to protected and sensitive information

"Data supply chain security is every corporation's responsibility"

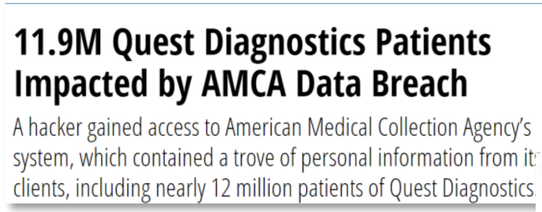


Drivers

Regulations

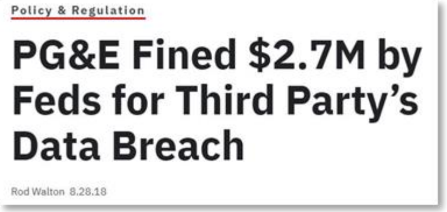


Data breaches caused by third-parties



11.9M Quest Diagnostics Patients Impacted by AMCA Data Breach

A hacker gained access to American Medical Collection Agency's system, which contained a trove of personal information from it clients, including nearly 12 million patients of Quest Diagnostics



Policy & Regulation

PG&E Fined $2.7M by Feds for Third Party's Data Breach

Rod Walton 8.28.18

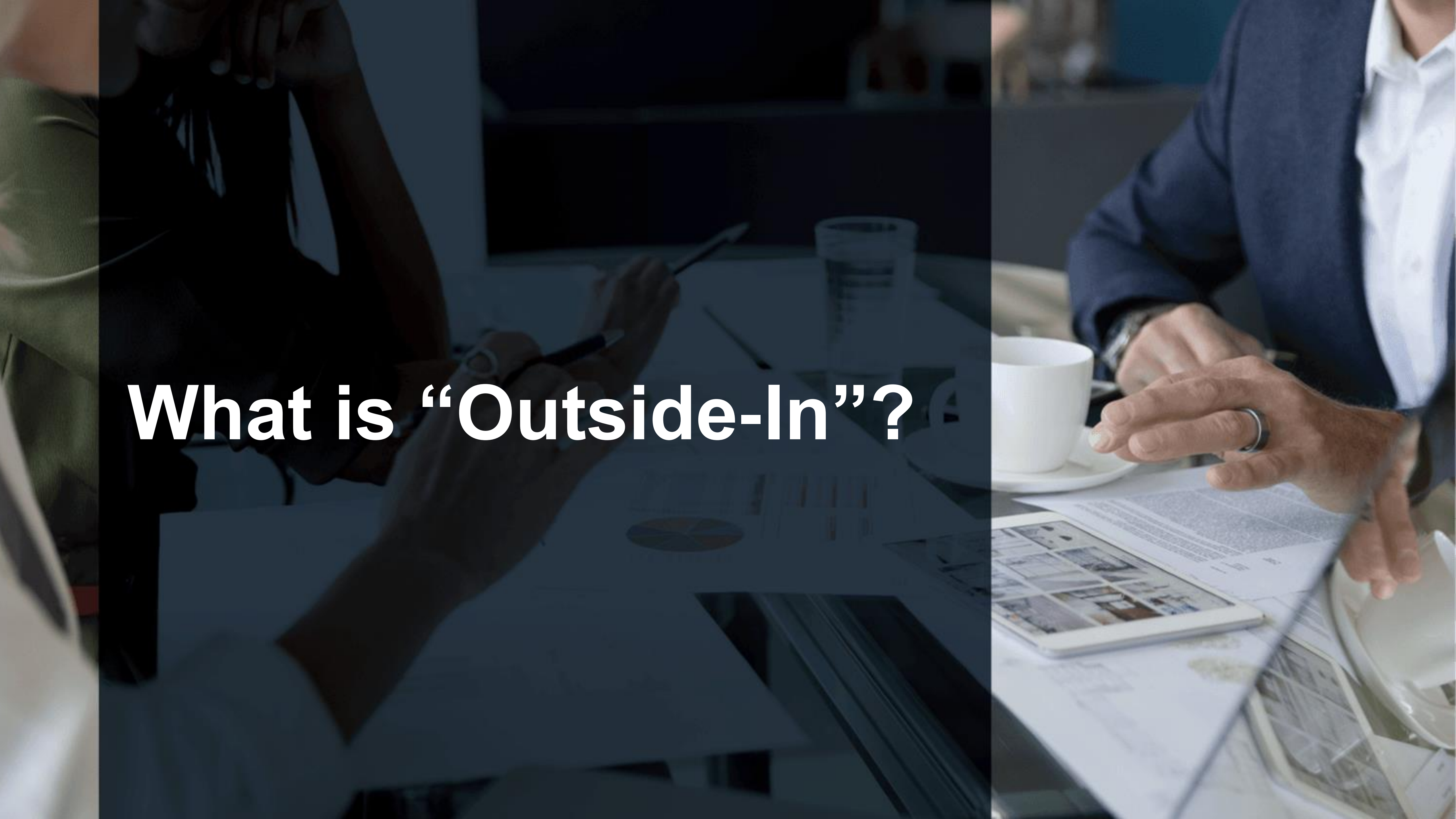
When?

- Before selection
- Onboarding
- Scope or role change
- Off-boarding

Some 3rd Party Related Data Breaches..

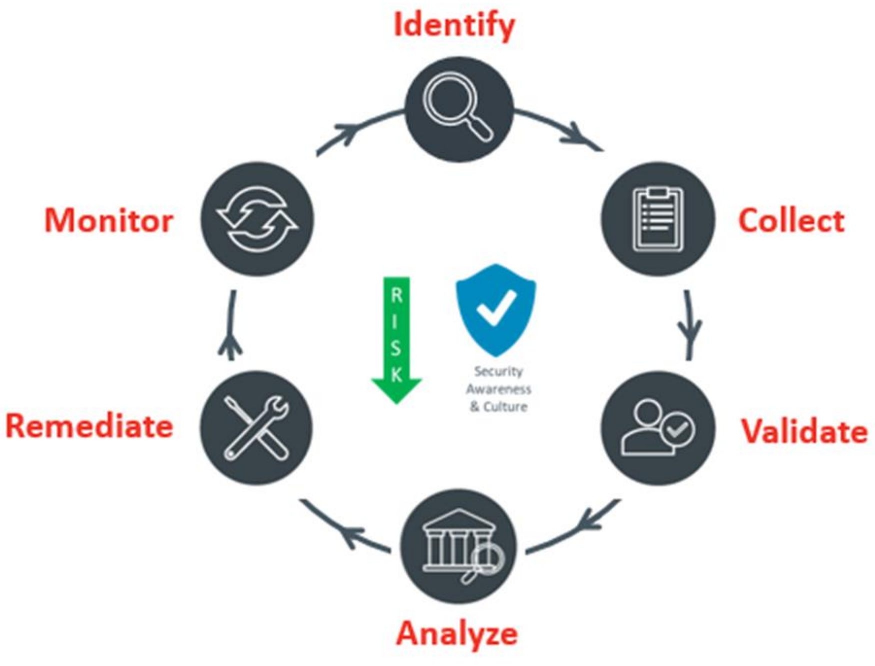
Reported in 2020

Date	Company
June	“BlueLeaks” (Netsential), Keepnet Labs
May	Florida Dept of Economic Activity, TrueCaller
April	Michigan State University, Marriott
March	Space X, Tesla, Boeing, PayPal, GE, T-Mobile
February	Idaho Central Credit Union, Carson City, Brunswick County Schools, TQL Carriers
January	Instagram, Regus, Mitsubishi, US State Governments



What is “Outside-In”?

The Cyber Risk Management Lifecycle



Cyber Risk Management Lifecycle (TPCRM)

At Identify / Collect decide:

- Who?
- What?
- How?

Inside-Out vs. Outside-In

Approach	Engage target to respond to questionnaire	Analyze externally available digital assets and data sources
Challenges	• Self-assessment, subject to ‘puffery’ • Velocity and scale	• Limited scope • Unclear beyond surface
Benefits	• Broader scope and deeper data • Understand cyber resilience	• Objective and easily scalable • Discrete – no engagement needed
Use Case	• M&A – Post Closing • Supply Chain – Critical Suppliers	• M&A – Pre-Closing • Supply Chain – Rest of Portfolio

Outside-In Scope and Approach

What do we look at?

Digital Footprint

Security Metrics

At-Risk Digital Identities

Objective:
Consistent data analysis, without influence from the organization, that can stand on its own and be evaluated in an absolute fashion

External:
Gathered from publicly viewable aspects of an organization’s IT infrastructure

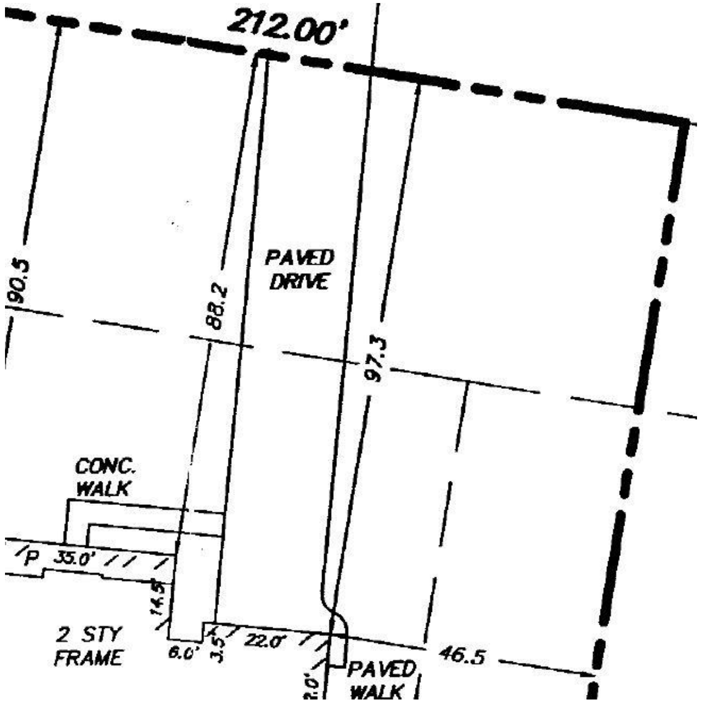
Discreet:
Passive scanning without organization knowledge. No illegal, unethical, or otherwise unallowed activity i.e. no ‘hacking’ or behind the firewall intrusion

Digital Footprint

- Identifies extent of organization’s ‘Attack Surface’

- Examines:
  - Domain registrations
  - Hosting Providers
  - Hosting Countries

- The “Property Lines” of the target organizations digital “Address”



Security Metrics

- Examines the objective data from the “Digital Address”
- Identifies known vulnerabilities, configuration issues, unpatched systems, or other material weaknesses
- Best to compare to others
  - You don’t want to be the worst looking house on the block…

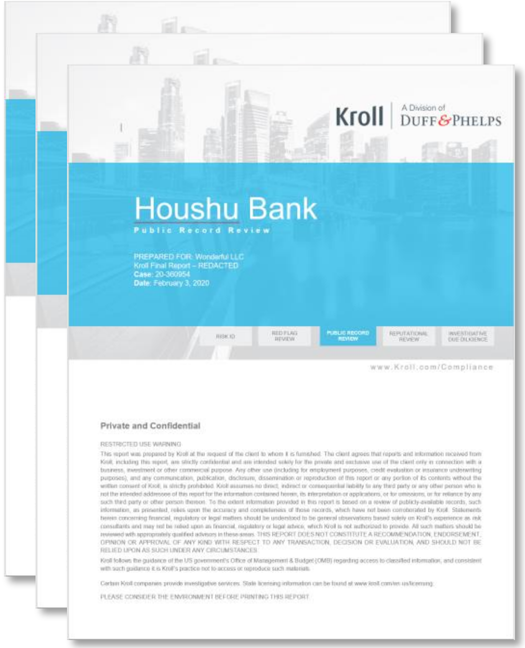
At-Risk Digital Identities

- Sources: Leaks, dumps, hacks, posts, or chats from forums, boards, web sites or other repositories
- Often data that is considered part of the "Dark Web"
- May be caused by a breach of the target organization, or a third-party related to it

Client Delivery

How our clients access Outside-In

Example Client Delivery Models



Houshu Bank

Public Record Review

PREPARED FOR: Wonderful LLC
Kroll Final Report – REDACTED
Case: 20-360954
Date: February 3, 2020

RISK ID | RED FLAG REVIEW | PUBLIC RECORD REVIEW | REPUTATIONAL REVIEW | INVESTIGATIVE DUE DILIGENCE

www.Kroll.com/Compliance

Private and Confidential

RESTRICTED USE WARNING

This report was prepared by Kroll at the request of the client to whom it is furnished. The client agrees that reports and information received from Kroll, including this report, are strictly confidential and are intended solely for the private and exclusive use of the client only in connection with a business, investment or other commercial purpose. Any other use (including for employment purposes, credit evaluation or insurance underwriting purposes), and any communication, publication, disclosure, dissemination or reproduction of this report or any portion of its contents without the written consent of Kroll, is strictly prohibited. Kroll assumes no direct, indirect or consequential liability to any third party or any other person who is not the intended addressee of this report for the information contained herein, its interpretation or applications, or for omissions, or for reliance by any such third party or other person thereon. To the extent information provided in this report is based on a review of publicly-available records, such information, as presented, relies upon the accuracy and completeness of those records, which have not been corroborated by Kroll. Statements herein concerning financial, regulatory or legal matters should be understood to be general observations based solely on Kroll's experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which Kroll is not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas. THIS REPORT DOES NOT CONSTITUTE A RECOMMENDATION, ENDORSEMENT, OPINION OR APPROVAL OF ANY KIND WITH RESPECT TO ANY TRANSACTION, DECISION OR EVALUATION, AND SHOULD NOT BE RELIED UPON AS SUCH UNDER ANY CIRCUMSTANCES.

Kroll follows the guidance of the US government's Office of Management & Budget (OMB) regarding access to classified information, and consistent with such guidance it is Kroll's practice not to access or reproduce such materials.

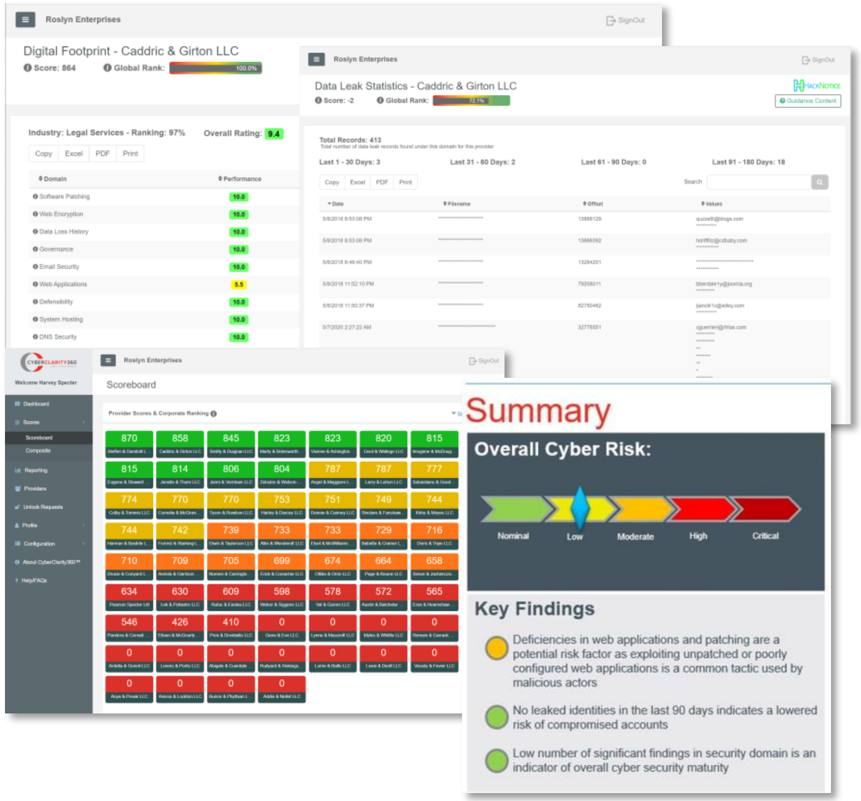
Certain Kroll companies provide investigative services. State licensing information can be found at www.kroll.com/en-us/licensing.

PLEASE CONSIDER THE ENVIRONMENT BEFORE PRINTING THIS REPORT.

Express

High Velocity, Scalable Portfolio Analysis

- Use our CyberClarity360 platform to objectively and discretely assess your target **portfolio**
- Compare cyber security posture across your **portfolio** and industry benchmarks
- Enhanced review of specific findings is available



Digital Footprint - Caddric & Girton LLC

Score: 864 Global Rank: 100.0%

Industry: Legal Services - Ranking: 97% Overall Rating: 9.4

Domain	Performance
Software Patching	10.0
Web Encryption	10.0
Data Loss History	10.0
Governance	10.0
Email Security	10.0
Web Applications	5.5
Defensibility	10.0
System Hosting	10.0
DNS Security	10.0

Data Leak Statistics - Caddric & Girton LLC

Score: -2 Global Rank: 72.1%

Total Records: 413

Total number of data leak records found under this domain for this provider

Last 1 - 30 Days: 3 Last 31 - 60 Days: 2 Last 61 - 90 Days: 0 Last 91 - 180 Days: 18

Date	Filename	Offset	Values
5/8/2018 8:53:08 PM	************************	13866129	quzzell@blogs.com ***********
5/8/2018 8:53:08 PM	************************	13866392	hdriffilz@cdbaby.com ***********
5/8/2018 8:46:40 PM	************************	13284201	****************************** ***********
5/8/2018 11:52:10 PM	************************	79208011	bberdale1y@joomla.org **********
5/8/2018 11:50:37 PM	************************	82750462	ljancik1v@wiley.com ***********
5/7/2020 2:27:22 AM	******************************	32776551	cguerrieri@rhtax.com ********** ********** ** ******** ** * ********

Scoreboard

Provider Scores & Corporate Ranking

870 Steffen & Dambold L...	858 Caddric & Girton LLC	845 Smitty & Duignan LLC	823 Marty & Bokesworth...	823 Vivienne & Ashington...	820 Cecil & Wallege LLC	815 Imogene & McDoug...
815 Eugene & Shawell...	814 Janelle & Thorn LLC	806 Jenni & Ventham LLC	804 Zebulon & Watson-...	787 Angel & Maggiore L...	787 Larry & Lehon LLC	777 Sebastiano & Good...
774 Colby & Tommis LLC	770 Cornelia & McGinn...	770 Tyson & Rowbon LLC	753 Harley & Darcey LLC	751 Donnie & Coiney LLC	749 Sinclare & Farshaw...	744 Kirby & Moyes LLC
744 Harman & Beslide L...	742 Forrest & Starking L...	739 Elwin & Taylorson LLC	733 Alin & Wendorolf LLC	733 Elsof & McWilliams...	729 Babette & Cramer L...	716 Doris & Tripe LLC
710 Drusie & Conyard L...	709 Antiola & Garrison...	705 Noreen & Carringto...	699 Erick & Conachie LLC	674 Ottilie & Orrin LLC	664 Page & Keane LLC	658 Simon & Jachimczu...
634 Pearson Specter Litt	630 Lek & Polisatro LLC	609 Rafus & Easles LLC	598 Weber & Siggons LLC	578 Val & Goroni LLC	572 Austin & Batchelor...	565 Evan & Hearnshaw...
546 Pandora & Cornell...	426 Eileen & McGoarty...	410 Pren & Dowdalls LLC	0 Gono & Eve LLC	0 Lynne & Mascroft LLC	0 Myles & Whittle LLC	0 Ronson & Carrack...
0 Ardella & Gonoll LLC	0 Lorees & Portis LLC	0 Abigale & Cuerdale...	0 Rudyard & Sekings...	0 Lorrie & Balle LLC	0 Lexie & Denil LLC	0 Vassily & Fewer LLC
0 Anya & Pesak LLC	0 Alessa & Lockton LLC	0 Buiron & Phythian L...	0 Addie & Nolet LLC			

Summary

Overall Cyber Risk:

Key Findings

- Deficiencies in web applications and patching are a potential risk factor as exploiting unpatched or poorly configured web applications is a common tactic used by malicious actors
- No leaked identities in the last 90 days indicates a lowered risk of compromised accounts
- Low number of significant findings in security domain is an indicator of overall cyber security maturity

Kroll Due Diligence

Value Proposition

Kroll | A Division of DUFF&PHELPS

Houshu Bank

Public Record Review

PREPARED FOR: Wonderful LLC
Kroll Final Report – REDACTED
Case: 20-360954
Date: February 3, 2020

www.Kroll.com/Compliance

Private and Confidential

RESTRICTED USE WARNING

This report was prepared by Kroll at the request of the client to whom it is furnished. The client agrees that reports and information received from Kroll, including this report, are strictly confidential and are intended solely for the private and exclusive use of the client only in connection with a business, investment or other commercial purpose. Any other use (including for employment purposes, credit evaluation or insurance underwriting purposes) and any communication, publication, disclosure, dissemination or reproduction of this report or any portion of its contents without the written consent of Kroll, is strictly prohibited. Kroll assumes no direct, indirect or consequential liability to any third party or any other person who is not the intended addressee of this report for the information contained herein, its interpretation or applications, or for omissions, or for reliance by any such third party or other person thereon. To the extent information provided in this report is based on a review of publicly-available records, such information, as presented, relies upon the accuracy and completeness of those records, which have not been corroborated by Kroll. Statements herein concerning financial, regulatory or legal matters should be understood to be general observations based solely on Kroll's experience as risk consultants and may not be relied upon as financial, regulatory or legal advice, which Kroll is not authorized to provide. All such matters should be reviewed with appropriately qualified advisors in these areas. THIS REPORT DOES NOT CONSTITUTE A RECOMMENDATION, ENDORSEMENT, OPINION OR APPROVAL OF ANY KIND WITH RESPECT TO ANY TRANSACTION, DECISION OR EVALUATION, AND SHOULD NOT BE RELIED UPON AS SUCH UNDER ANY CIRCUMSTANCES.

Kroll follows the guidance of the US government's Office of Management & Budget (OMB) regarding access to classified information, and consistent with such guidance it is Kroll's practice not to access or reproduce such materials.

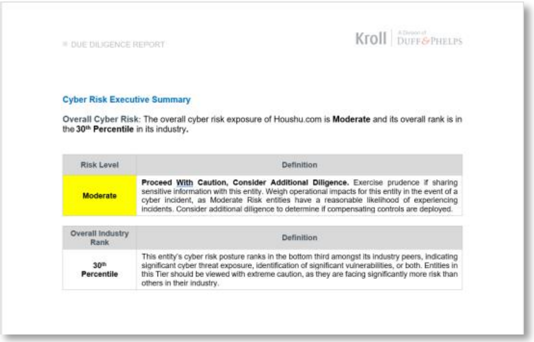
Certain Kroll companies provide investigative services. State licensing information can be found at www.kroll.com/en-us/licensing.

PLEASE CONSIDER THE ENVIRONMENT BEFORE PRINTING THIS REPORT.

- **Empowering** Clients to rapidly perform cyber risk diligence on existing or potential key partners
- **Enabling** Clients to understand a Target’s cybersecurity posture without their engagement
- **Delivering** key risk findings and actionable mitigation recommendations for M&A and supply chain

Kroll Cyber Risk Report Structure

Executive Summary



Kroll | A Division of DUFF & PHELPS

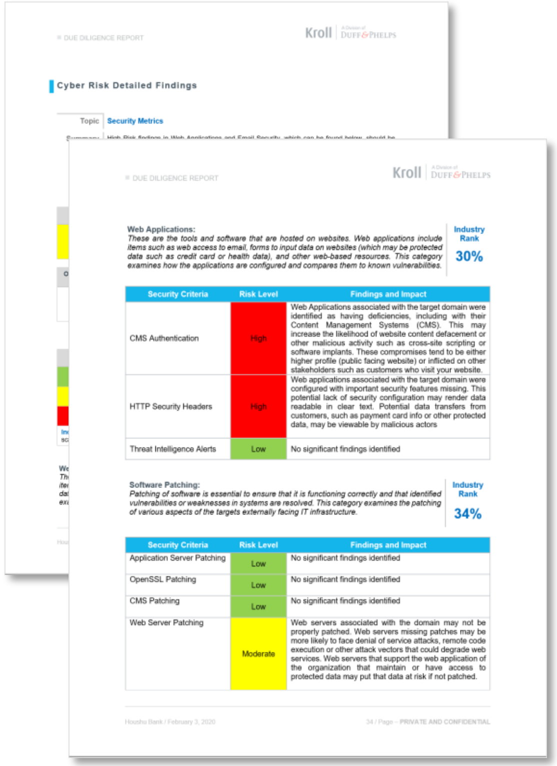
Cyber Risk Executive Summary

Overall Cyber Risk: The overall cyber risk exposure of Houshu.com is **Moderate** and its overall rank is in the **30th Percentile** in its industry.

Risk Level	Definition
Moderate	**Proceed With Caution, Consider Additional Diligence.** Exercise prudence if sharing sensitive information with this entity. Weigh operational impacts for this entity in the event of a cyber incident, as Moderate Risk entities have a reasonable likelihood of experiencing incidents. Consider additional diligence to determine if compensating controls are deployed.

Overall Industry Rank	Definition
30th Percentile	This entity's cyber risk posture ranks in the bottom third amongst its industry peers, indicating significant cyber threat exposure, identification of significant vulnerabilities, or both. Entities in this Tier should be viewed with extreme caution, as they are facing significantly more risk than others in their industry.

Security Metrics



Kroll | A Division of DUFF & PHELPS

Cyber Risk Detailed Findings

Topic: **Security Metrics**

Summary: High Risk findings in Web Applications and Email Security, which can be found below, should be

Kroll | A Division of DUFF & PHELPS

Web Applications:
These are the tools and software that are hosted on websites. Web applications include items such as web access to email, forms to input data on websites (which may be protected data such as credit card or health data), and other web-based resources. This category examines how the applications are configured and compares them to known vulnerabilities.

Industry Rank **30%**

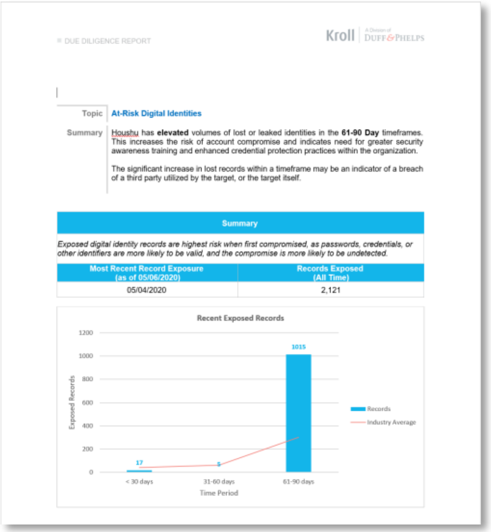
Security Criteria	Risk Level	Findings and Impact
CMS Authentication	High	Web Applications associated with the target domain were identified as having deficiencies, including with their Content Management Systems (CMS). This may increase the likelihood of website content defacement or other malicious activity such as cross-site scripting or software implants. These compromises tend to be either higher profile (public facing website) or inflicted on other stakeholders such as customers who visit your website.
HTTP Security Headers	High	Web applications associated with the target domain were configured with important security features missing. This potential lack of security configuration may render data readable in clear text. Potential data transfers from customers, such as payment card info or other protected data, may be viewable by malicious actors
Threat Intelligence Alerts	Low	No significant findings identified

Software Patching:
Patching of software is essential to ensure that it is functioning correctly and that identified vulnerabilities or weaknesses in systems are resolved. This category examines the patching of various aspects of the targets externally facing IT infrastructure.

Industry Rank **34%**

Security Criteria	Risk Level	Findings and Impact
Application Server Patching	Low	No significant findings identified
OpenSSL Patching	Low	No significant findings identified
CMS Patching	Low	No significant findings identified
Web Server Patching	Moderate	Web servers associated with the domain may not be properly patched. Web servers missing patches may be more likely to face denial of service attacks, remote code execution or other attack vectors that could degrade web services. Web servers that support the web application of the organization that maintain or have access to protected data may put that data at risk if not patched.

At-Risk Digital Identities



Kroll | A Division of DUFF & PHELPS

Topic: **At-Risk Digital Identities**

Summary: Houshu has **elevated** volumes of lost or leaked identities in the **61-90 Day** timeframes. This increases the risk of account compromise and indicates need for greater security awareness training and enhanced credential protection practices within the organization.

The significant increase in lost records within a timeframe may be an indicator of a breach of a third party utilized by the target, or the target itself.

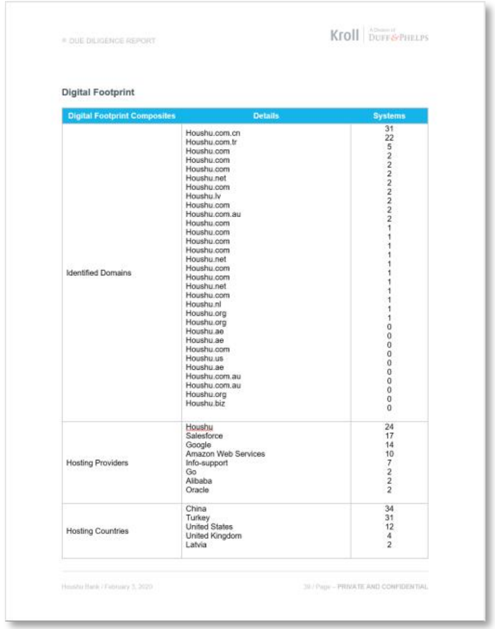
Summary

Exposed digital identity records are highest risk when first compromised, as passwords, credentials, or other identifiers are more likely to be valid, and the compromise is more likely to be undetected.

Most Recent Record Exposure (as of 05/06/2020)	Records Exposed (All Time)
05/04/2020	2,121

Recent Exposed Records

Digital Footprint



Kroll | A Division of DUFF & PHELPS

Digital Footprint

Digital Footprint Composites	Details	Systems
Identified Domains	Houshu.com.cn Houshu.com.tr Houshu.com Houshu.com Houshu.com Houshu.net Houshu.com Houshu.lv Houshu.com Houshu.com.au Houshu.com Houshu.com Houshu.com Houshu.com Houshu.net Houshu.com Houshu.com Houshu.net Houshu.com Houshu.nl Houshu.org Houshu.org Houshu.ae Houshu.ae Houshu.com Houshu.us Houshu.ae Houshu.com.au Houshu.com.au Houshu.org Houshu.biz	31 22 5 2 2 2 2 2 2 2 2 1 1 1 1 1 1 1 1 1 1 1 0 0 0 0 0 0 0 0 0 0
Hosting Providers	Houshu Salesforce Google Amazon Web Services Info-support Go Alibaba Oracle	24 17 14 10 7 2 2 2
Hosting Countries	China Turkey United States United Kingdom Latvia	34 31 12 4 2

Thank You

For more information please contact:

Imran Jaswal

Imran.Jaswal@duffandphelps.com

M: +1 (858) 231-4948

Kevin Braine

Kevin.Braine@Kroll.com

M: +44 7880 475264

Ryan Spelman

Ryan.Spelman@duffandphelps.com

M: +1 (518) 257-6357

CYBERCLARITY360
A DUFF & PHELPS PRODUCT