Integrating 3rd Party Scoring Services into your Enterprise KRIs

A Year of Lessons Learned

Joe Corsi
Sr. Manager, Enterprise Security
Paychex Inc.

Tony Karakashian
Project Lead, Enterprise Security
Paychex Inc.

PAYCHEX®

Agenda

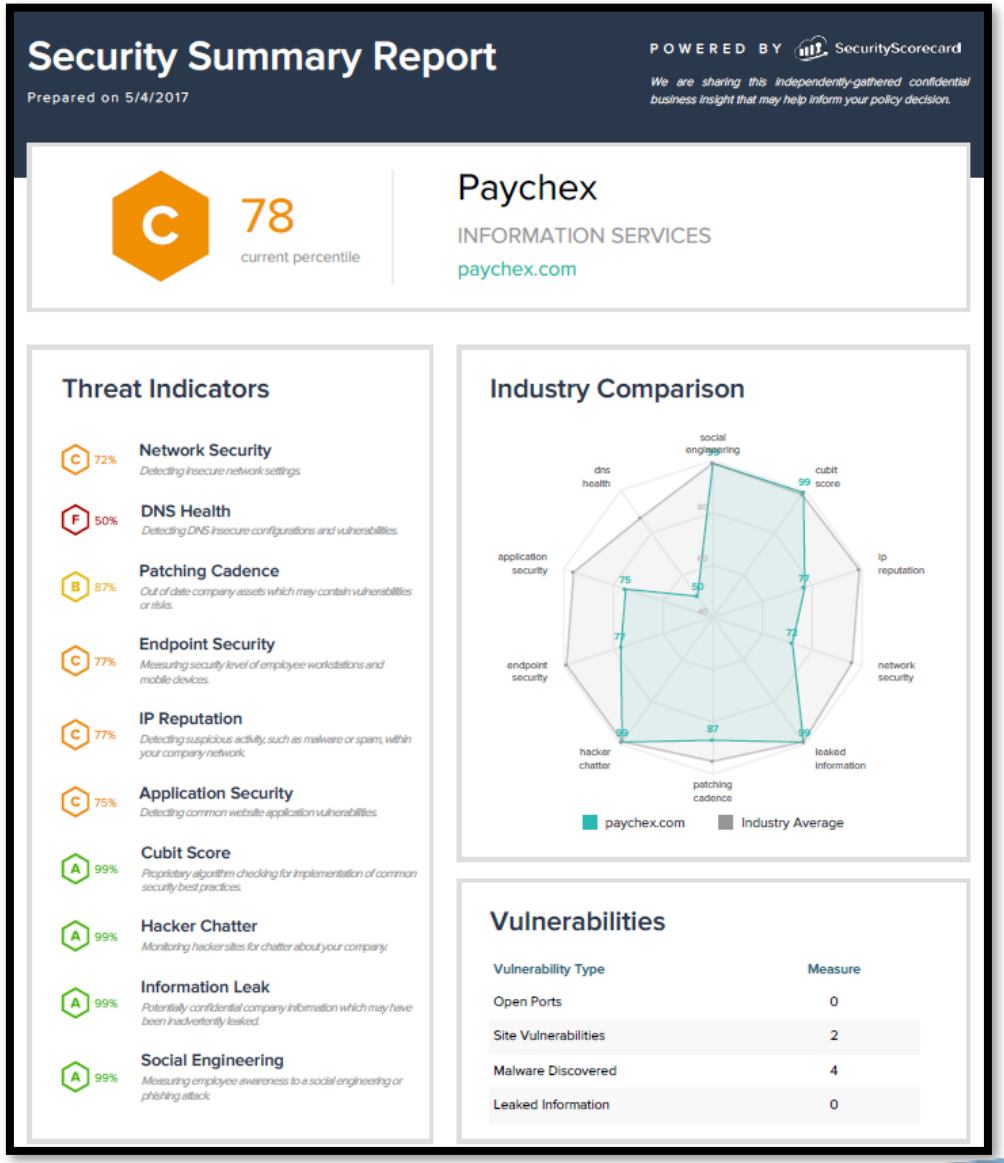
- Quick story
- Why This Is Important
- How the Scoring is Gather and Calculated
- Different Types of Reporting
- How We’ve Implemented Scoring into our Security Teams
- Lessons Learned – A Year Later
- Questions

A Brief Story a Year in the Making

- Contacted by a perspective client that we did not have a very good score and could not move forward with evaluation
- Asked to go through our report and provide remediation actions for each finding
- Quickly identified there were some false positives
- Significant work put forth to put together a project plan for legitimate gaps
- Ultimately deal was signed and everyone was happy

This caused us to re-evaluate two things:

1. Should we be using this for our vendors?
2. Shouldn't we be aware of our score at all times?



So, what are we talking about here…

"We think that at some point in the near term, a *cybersecurity score will be as important as a credit score* when organizations look to sign up for a partnership."

Jeffrey Wheatman, Research Director, Security and Privacy, at Gartner

How I explained it to my CEO: the home assessor example

How these scores are calculated

The biggest security-score providers only analyze a company's security posture using externally accessible data that they don't need permission to acquire

The real differentiator, or "secret sauce," is the vendor's depth of collected data and the analytics it uses to come up with a score, which can be hard to discern

Security-score providers use their own unique scales. Can range from 0 to 900 or a letter grade A through F based on 'x' security domains

Providers attempt to create value by predicting a company's likelihood of a significant breach within the next 12 months

What's in a Security Score?

External surveillance of a company's security practices

- Vulnerabilities to active gateways
- Encryption
- Multi-factor authentication
- Patching frequency
- File sharing practices
- Leaked credentials found on the web
- Spam propagation
- Open ports

Publicly available intelligence

- Open source malware intelligence
- Subscription Threat intelligence data feeds
- Hacker/Dark Web chatter

Secret Sauce

- Historical data collected to establish behavior patterns
- Proprietary algorithms

Material provided by CSO Online : https://www.csoonline.com/article/3103293/security/what-s-in-a-security-score.html

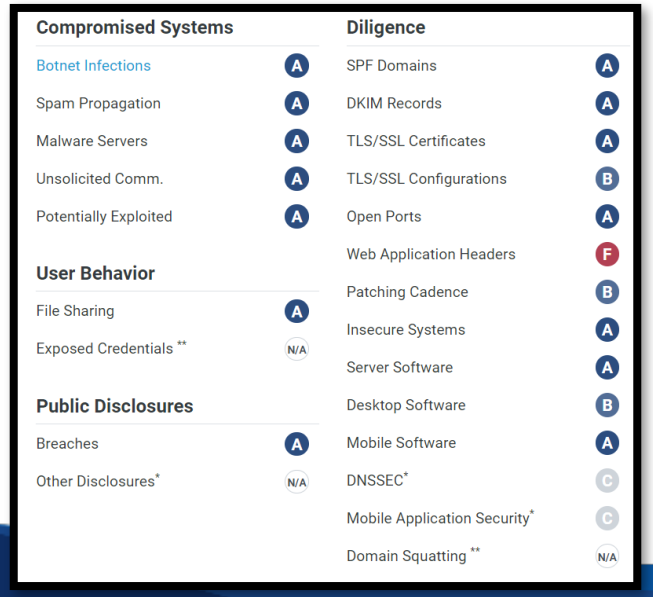
So what can they actually see…

- Network Security – TLS/SSL Certificates, TLS/SSL Configurations, Open Ports etc.
- DNS Health – Domain Management, SPF Records, DKIM Records
- Patching Cadence – Vulnerabilities, End-of-life services
- Endpoint Security – Outdated OS and web browsers, Desktop, Mobile, and Server Software
- Insecure Systems – Botnet infections, spam propagation
- IP Reputation – Malware analysis
- Application Security – Site HTTPS, Content Mgmt. Vulnerabilities, Web Application Headers
- Information on “Dark Web” – Hacker chatter, leaked credentials

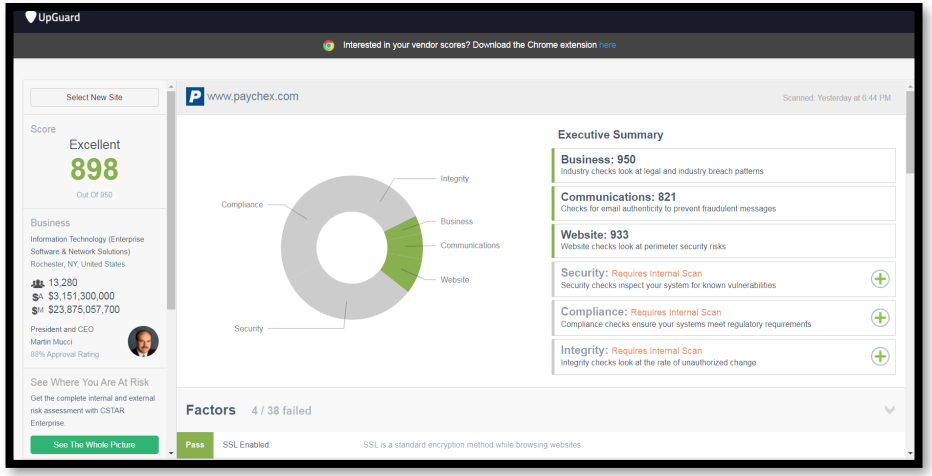
Each provider may have different scoring, weighting, and possibly measured against “industry peers”

Many Vendors, Different Types of Reporting

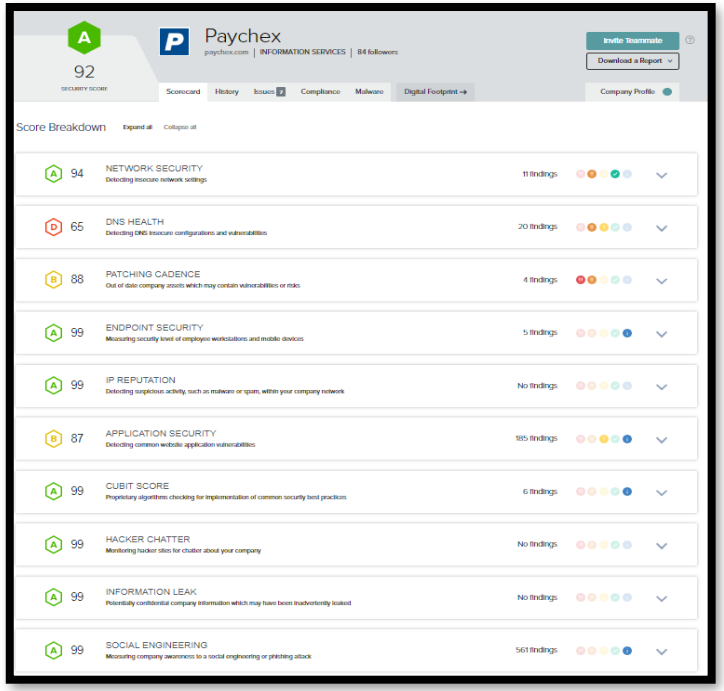
BitSight

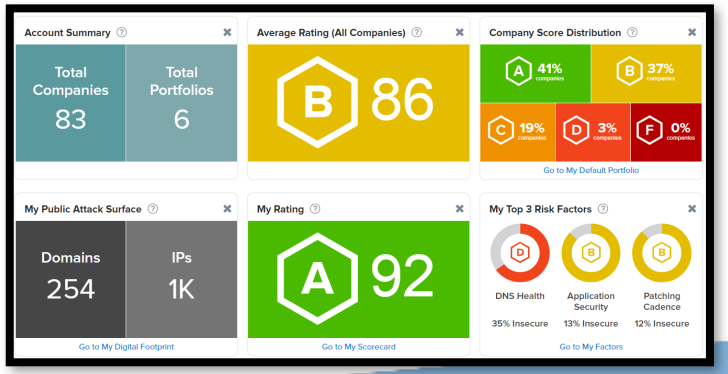


Upguard



SecurityScorecard





How We Use These Metrics

Our Footprint

- Decided to use two different vendors to ensure accuracy; will re-evaluate year-to-year
- Both vendors score our company, our subsidiaries, and our competition (roughly 15-20 slots)
- One vendor also scores our key service providers (aka critical vendors; roughly 50 additional slots)
- Does not supplant our other vendor processes (questionnaires, on-site visits, etc.)

Functions

- Triage and Remediation of own Findings
- Vendor Risk Measurement and Follow-Up
- Audit Evidence and Client Response Questionnaires
- Merger and Acquisition Measurement
- Monthly Reporting to Measure Progress

What your Board will use them for…

Competitive Analysis

Company Comparison

	You	Competitors			
Security Rating February 17, 2018	780 Advanced	600 Basic	610 Basic	770 Advanced	780 Advanced
52 week range	720 - 810	530 - 600	590 - 620	750 - 770	700 - 780
Compromised Systems					
Botnet Infections	A	D	C	A	A
Spam Propagation	A	C	D	A	A
Malware Servers	A	A	A	A	A
Unsolicited Comm.	A	A	A	A	A
Potentially Exploited	A	F	D	A	A
Diligence					
SPF	B	A	C	B	A
DKIM	A	A	B	B	B
SSL Certificates	A	B	B	C	D

Market Differentiation

7 companies

Print to PDF

FACTORS	You	Competitors					
	A 91	C 79	A 90	C 75	A 92	B 88	A 92
Network Security	A 99	B 81	A 93	D 68	B 83	B 85	A 98
DNS Health	D 65	F 50	D 62	F 52	A 99	C 70	B 88
Patching Cadence	C 79	C 75	B 84	C 73	C 71	A 95	C 73
Endpoint Security	A 99	C 71	A 99	C 77	A 99	C 78	B 86
IP Reputation	A 99	A 95	A 99	B 84	A 99	A 99	A 99
Application Security	B 87	F 58	C 74	F 51	A 99	D 67	A 91
Cubit Score	A 99	A 96	A 99	B 86	A 98	A 99	A 99
Hacker Chatter	A 99	A 99	A 99	A 99	A 99	A 99	A 99
Information Leak	A 99	A 99	A 99	A 99	A 99	A 99	A 99
Social Engineering	A 99	A 99	A 99	A 99	A 99	A 99	A 99

Be Ready For This!

How We've Implemented Scoring into each Function

Triage and Remediation of own Findings

- Project team dedicated to watching and remediation
- Verified to determine false positive or not
- Triaged appropriately to determine mitigation path and priority

Vendor Risk Measurement and Follow-Up

- Critical vendors only
- Determine a threshold at which point follow-up is needed; based on time and personnel
- Does not replace other vendor actions; only supplements

How We've Implemented Scoring into each Function

Merger and Acquisition Risk Measurement

- Good "first look" at a company's security posture
- Also, may provide some guidance on external IP space for your own security scanning
- Allows for a more prepared on-site discussion if needed

Client Audit Artifact

- Provide as a artifact to demonstrate adherence to some controls
- Can provide either a summary report, or more detailed depending on your level of comfortability

Monthly Reporting to Measure Progress

- Out-of-box reporting does exist, but not always where you want to focus
- Ensure decision-makers understand meaning of fluctuations in scoring

Lessons Learned – A Year Later

Pitfalls and Challenges

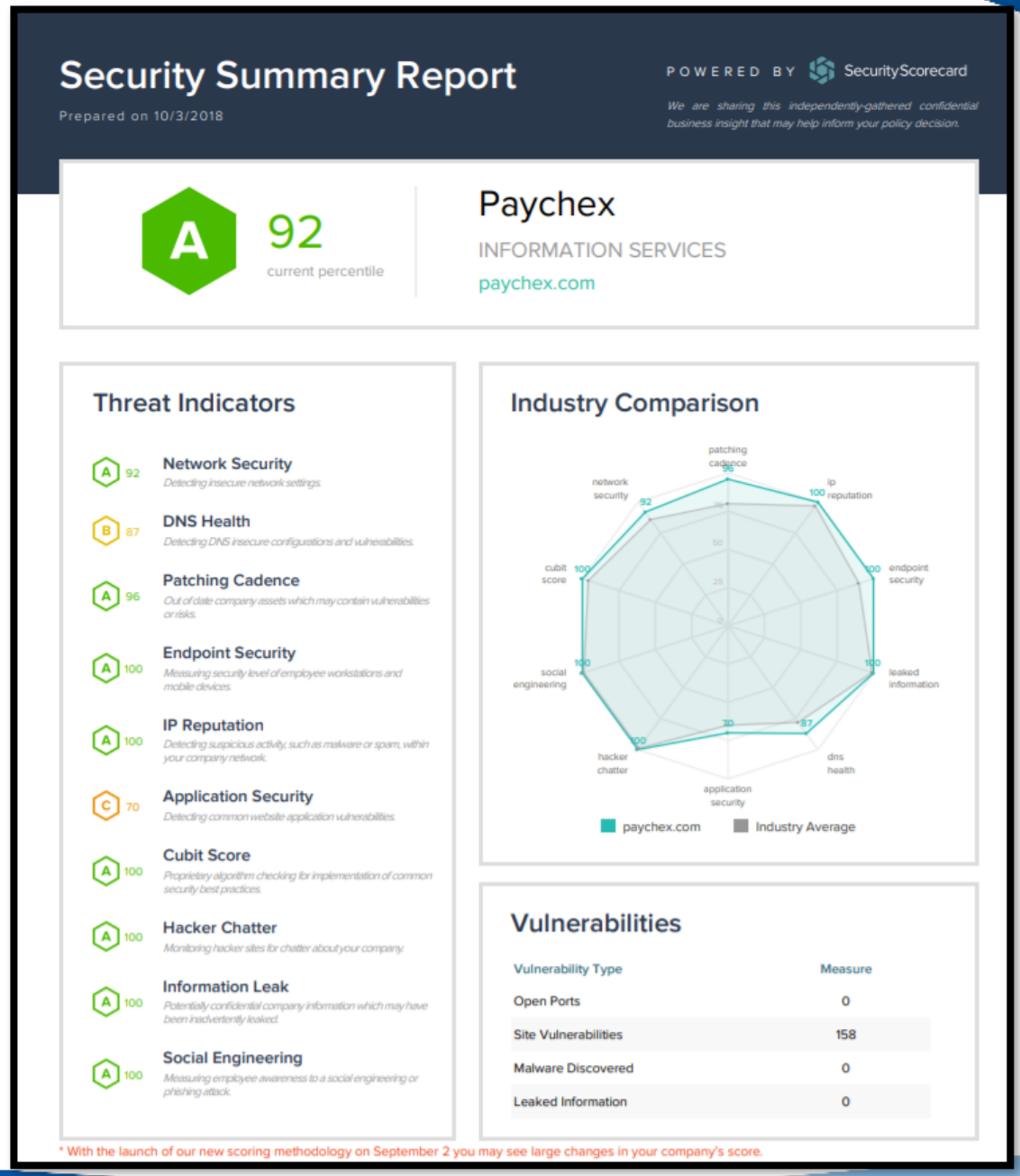
- Volatility of scoring
- Cost and number of providers
- False Positives
- Technologist Buy-In; before the fire-drill

Recommendations

- Gain early buy-in from cross-functional teams
- Set clear expectations to Sr. Management
- Form relationship with your chosen vendor
- Designate a team/person to be responsible for monitoring, triage, and remediation of findings

Our Score Today

Still working on how to market this



Security Summary Report

Prepared on 10/3/2018

POWERED BY SecurityScorecard

We are sharing this independently-gathered confidential business insight that may help inform your policy decision.

A 92 current percentile

Paychex

INFORMATION SERVICES

paychex.com

Threat Indicators

- A 92 **Network Security** — *Detecting insecure network settings.*
- B 87 **DNS Health** — *Detecting DNS insecure configurations and vulnerabilities.*
- A 96 **Patching Cadence** — *Out of date company assets which may contain vulnerabilities or risks.*
- A 100 **Endpoint Security** — *Measuring security level of employee workstations and mobile devices.*
- A 100 **IP Reputation** — *Detecting suspicious activity, such as malware or spam, within your company network.*
- C 70 **Application Security** — *Detecting common website application vulnerabilities.*
- A 100 **Cubit Score** — *Proprietary algorithm checking for implementation of common security best practices.*
- A 100 **Hacker Chatter** — *Monitoring hacker sites for chatter about your company.*
- A 100 **Information Leak** — *Potentially confidential company information which may have been inadvertently leaked.*
- A 100 **Social Engineering** — *Measuring employee awareness to a social engineering or phishing attack.*

Industry Comparison

Vulnerabilities

Vulnerability Type	Measure
Open Ports	0
Site Vulnerabilities	158
Malware Discovered	0
Leaked Information	0

* With the launch of our new scoring methodology on September 2 you may see large changes in your company's score.

Questions?

Joe Corsi
Sr. Manager, Enterprise Security
Paychex Inc.
jcorsi@paychex.com

Tony Karakashian
Project Lead, Enterprise Security
Paychex Inc.
akarakashian@paychex.com

Sources Used

www.securityscorecard.com
www.bitsight.com
www.upguard.com
www.csoonline.com
www.techrepubliccom