Measuring the Cyber Attack Surface

Jon Ehret, VP of Strategy & Risk @ RiskRecon

Wade Baker, Partner @ Cyentia Institute

riskrecon

mastercard

State of Third-Party Risk Management 2020

STATE OF
THIRD-PARTY RISK
MANAGEMENT 2020

A collaborative research project between RiskRecon and the Cyentia Institute

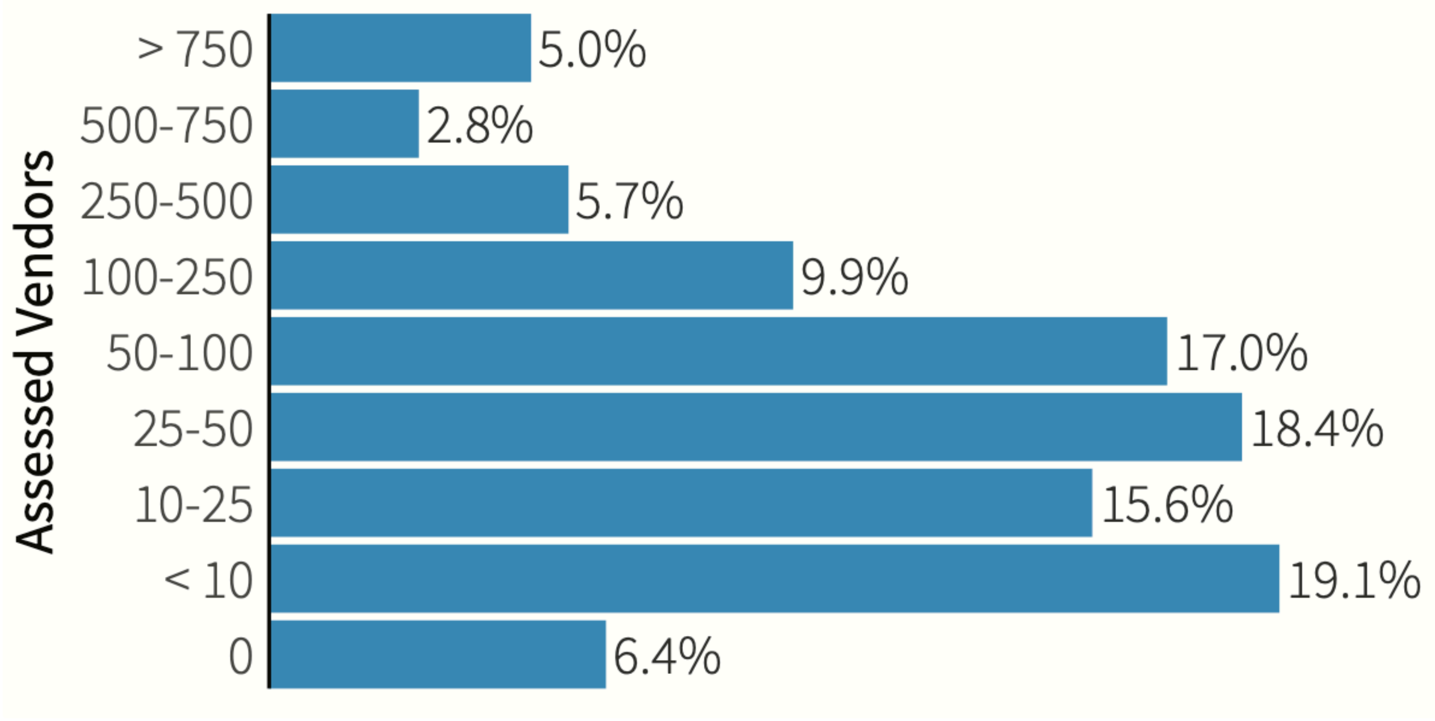
riskrecon mastercard

Cyentia INSTITUTE

- Aims to understand the challenges currently faced by TPRM programs, examine what they're doing to meet those challenges, and identify factors that improve their chance of success.
- Input from 150+ vetted TPRM professionals, primarily via workshops run by RiskRecon in 2020

How many active vendors under management?

FIGURE 1: NUMBER OF VENDORS RECEIVING CYBER RISK ASSESSMENTS EACH YEAR (PER FIRM)



1 in 3 TPRM programs assess

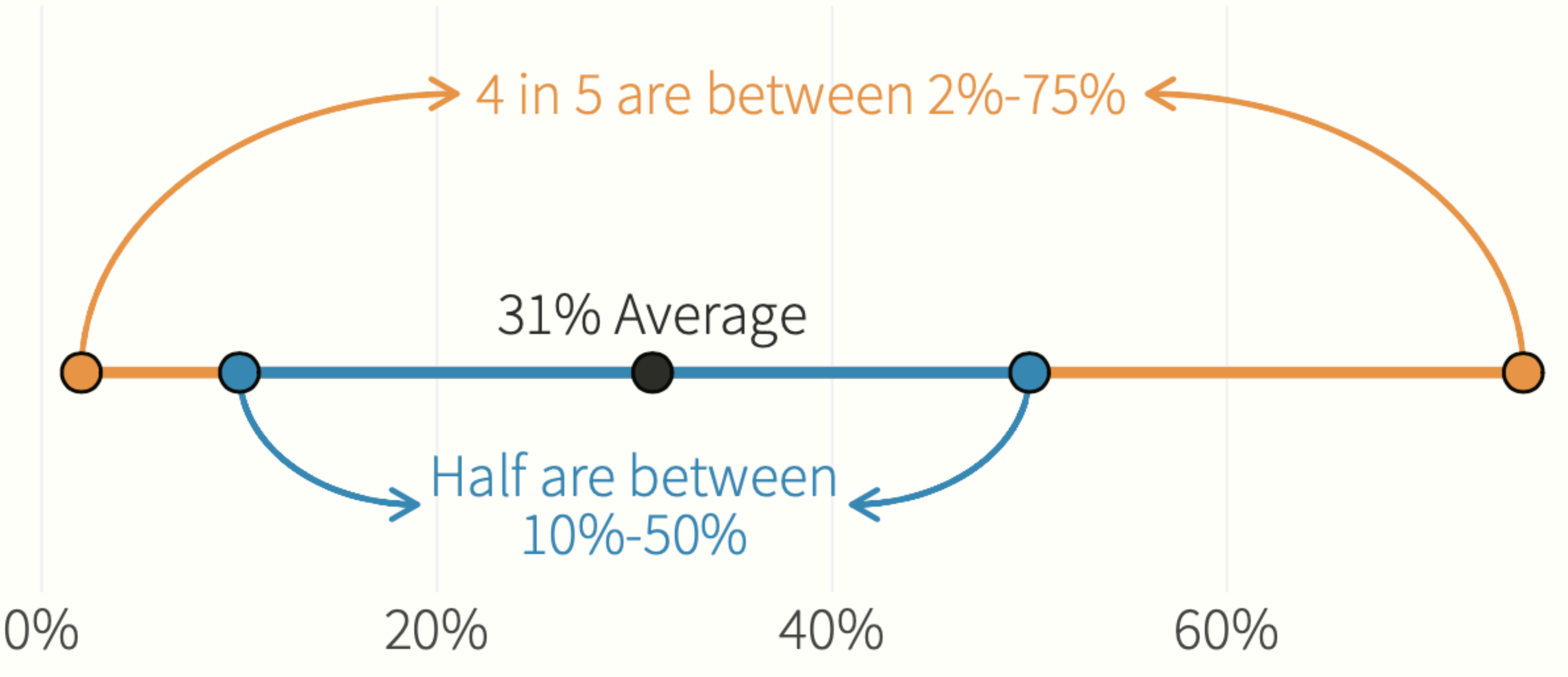
100+

vendors per year

riskrecon mastercard

How many vendors represent material risk?

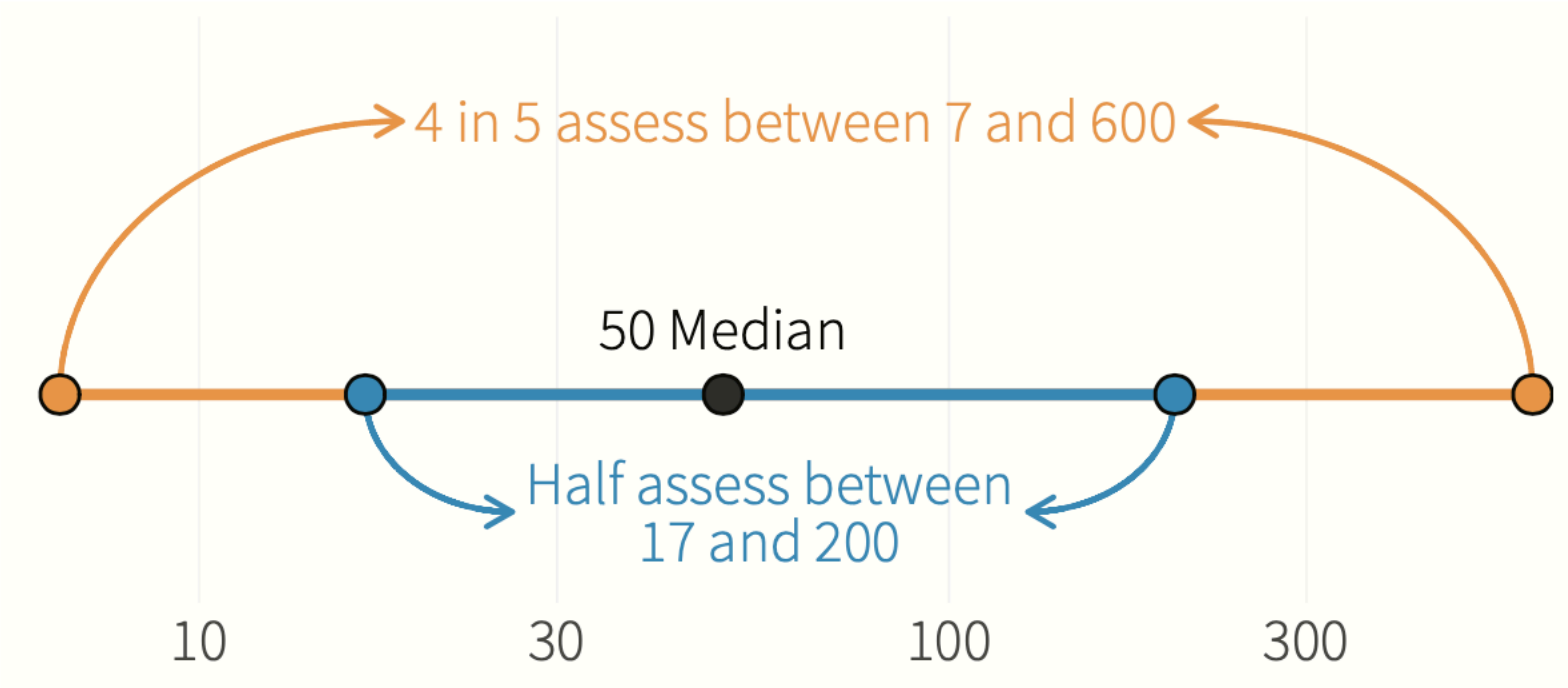
FIGURE 2: PERCENT OF VENDORS THAT COULD CAUSE CRITICAL IMPACT FROM CYBER EVENTS



31% of vendors considered a material risk in the event of a breach

What’s the vendor-to-staff ratio for TPRM assessments?

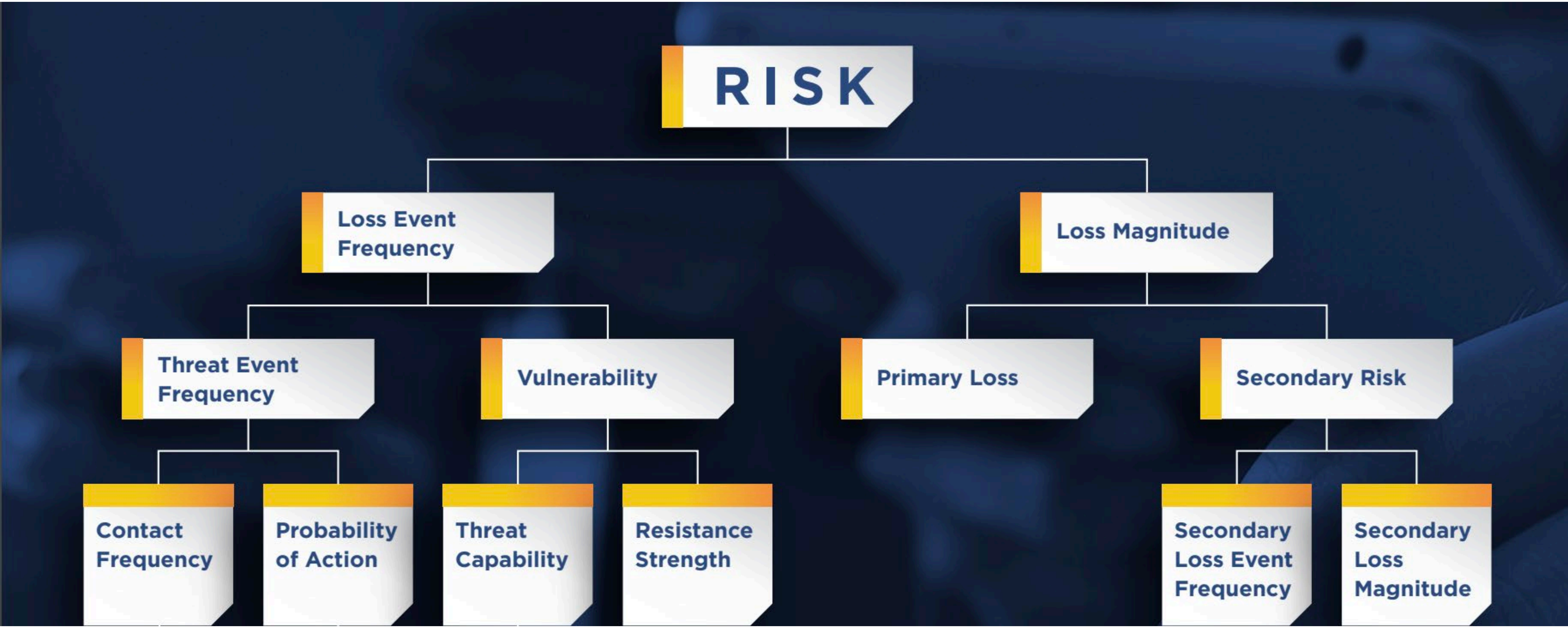
FIGURE 8: NUMBER OF VENDORS ASSESSED ANNUALLY PER FTE



TPRM programs typically manage **50** vendors per FTE

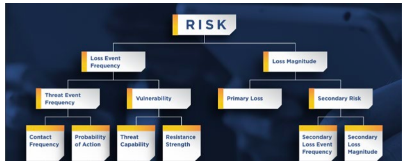
Enterprise cyber risk assessments are hard…

Thankfully, we have good frameworks like FAIR™ to help

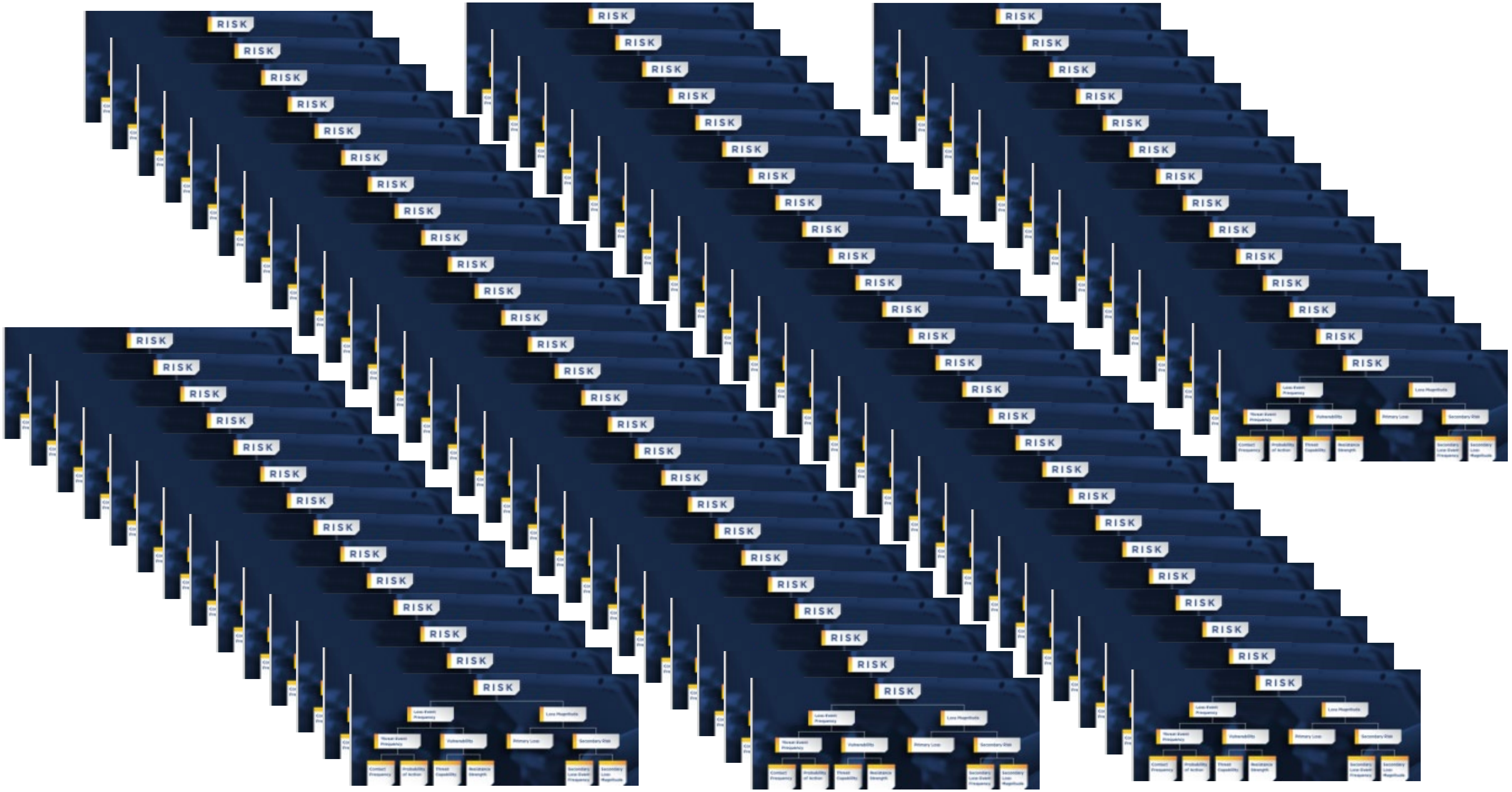


…but they don't scale well across 3rd parties…

Your firm

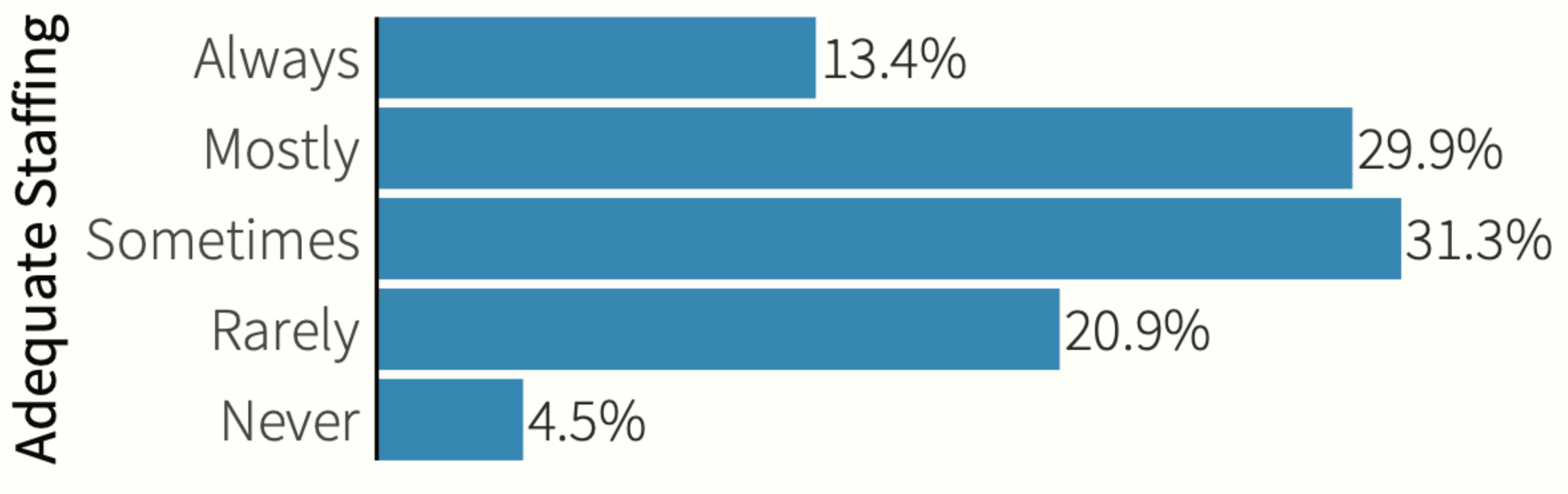


Your firm's network of 3rd parties



TPRM programs are overwhelmed

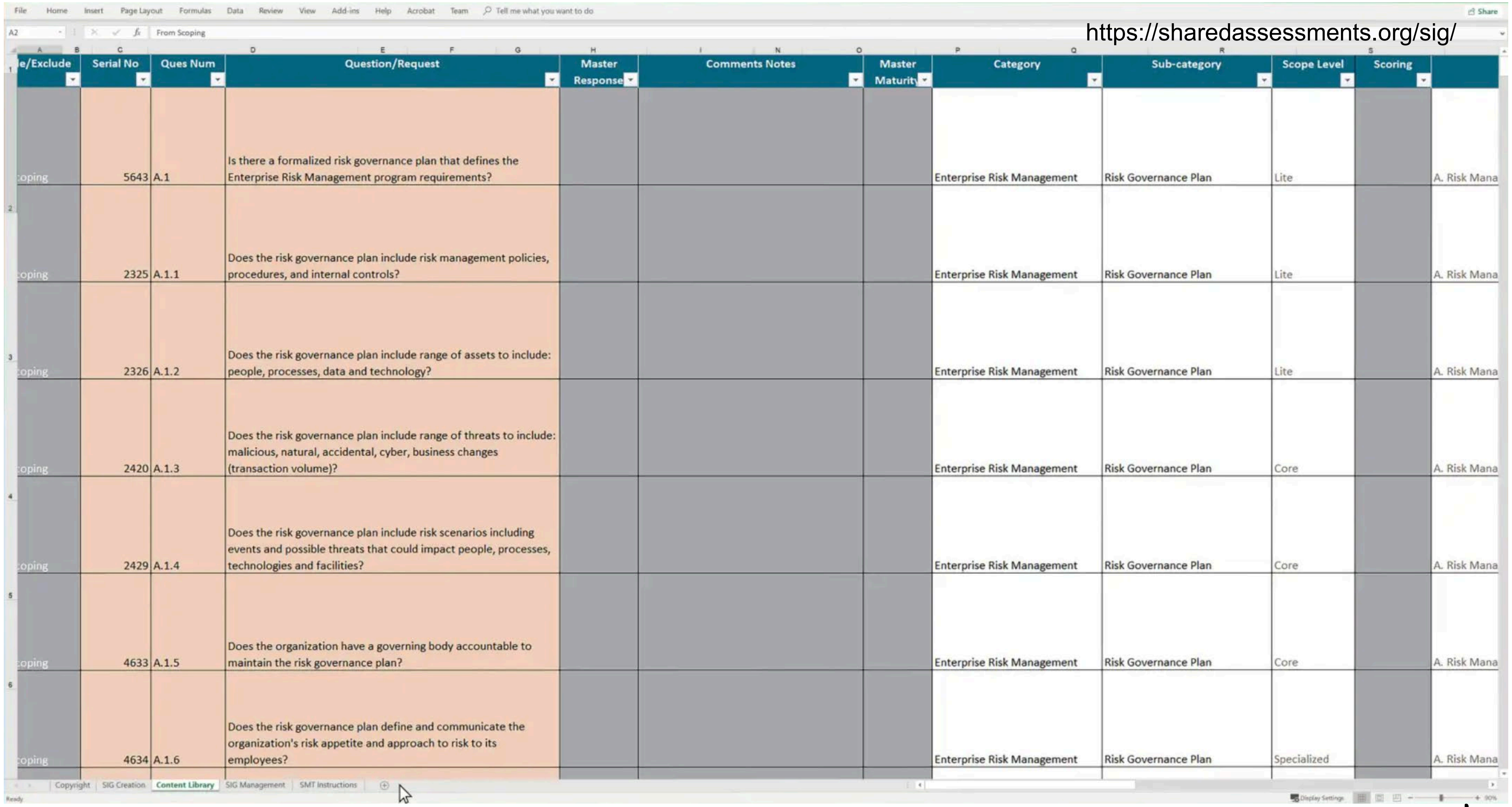
FIGURE 9: PERCENT OF RESPONDENTS WHO REPORT TPRM STAFFING IS ADEQUATE



87%

report inadequate TPRM staffing

…so we do what we can with what we have…

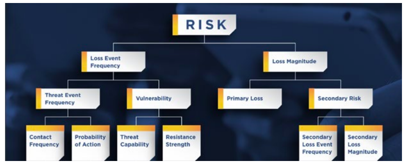


https://sharedassessments.org/sig/

le/Exclude	Serial No	Ques Num	Question/Request	Master Response	Comments Notes	Master Maturity	Category	Sub-category	Scope Level	Scoring	
coping	5643	A.1	Is there a formalized risk governance plan that defines the Enterprise Risk Management program requirements?				Enterprise Risk Management	Risk Governance Plan	Lite		A. Risk Mana
coping	2325	A.1.1	Does the risk governance plan include risk management policies, procedures, and internal controls?				Enterprise Risk Management	Risk Governance Plan	Lite		A. Risk Mana
coping	2326	A.1.2	Does the risk governance plan include range of assets to include: people, processes, data and technology?				Enterprise Risk Management	Risk Governance Plan	Lite		A. Risk Mana
coping	2420	A.1.3	Does the risk governance plan include range of threats to include: malicious, natural, accidental, cyber, business changes (transaction volume)?				Enterprise Risk Management	Risk Governance Plan	Core		A. Risk Mana
coping	2429	A.1.4	Does the risk governance plan include risk scenarios including events and possible threats that could impact people, processes, technologies and facilities?				Enterprise Risk Management	Risk Governance Plan	Core		A. Risk Mana
coping	4633	A.1.5	Does the organization have a governing body accountable to maintain the risk governance plan?				Enterprise Risk Management	Risk Governance Plan	Core		A. Risk Mana
coping	4634	A.1.6	Does the risk governance plan define and communicate the organization's risk appetite and approach to risk to its employees?				Enterprise Risk Management	Risk Governance Plan	Specialized		A. Risk Mana

…but even that doesn't scale (or assess risk) well.

Your firm



Your firm's network of 3rd parties

Lack of confidence and action from questionnaires

FIGURE 16: DO YOU BELIEVE VENDOR RESPONSES?

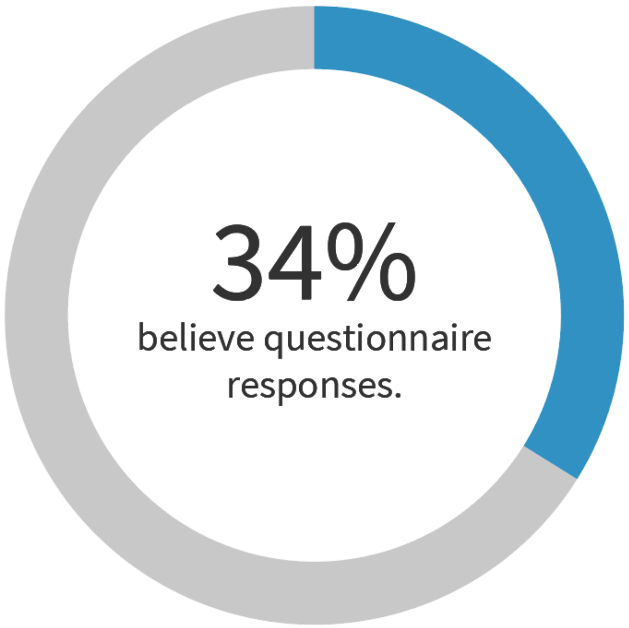


FIGURE 14: DO YOU REQUIRE VENDOR REMEDIATION?

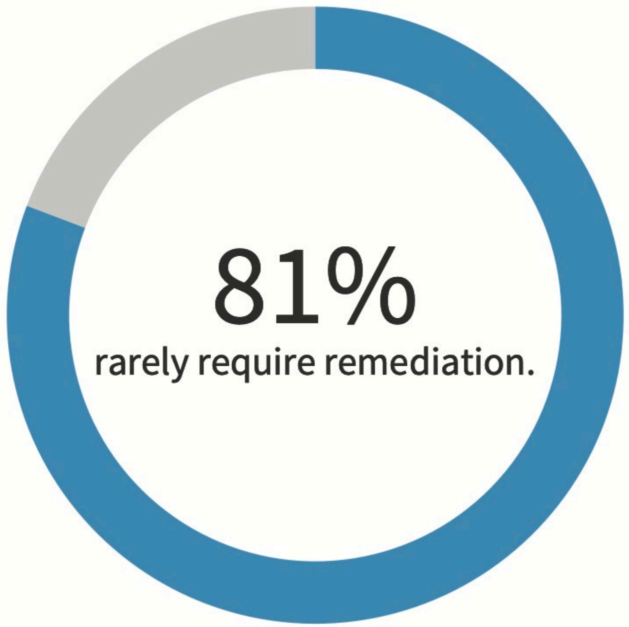
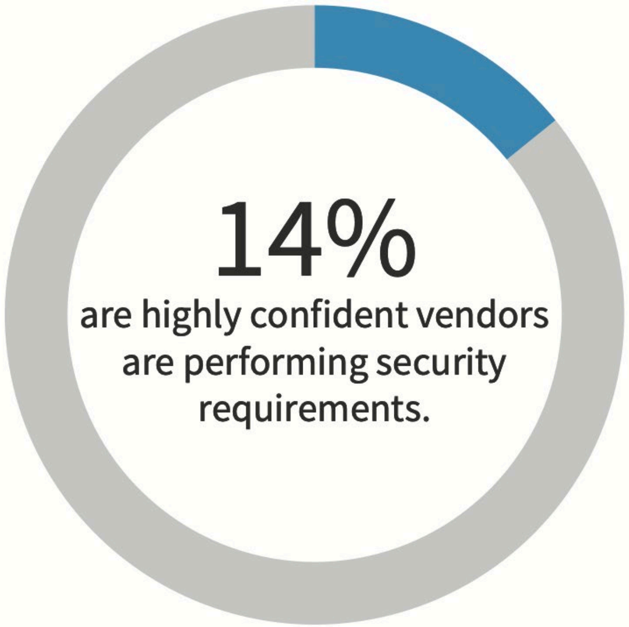
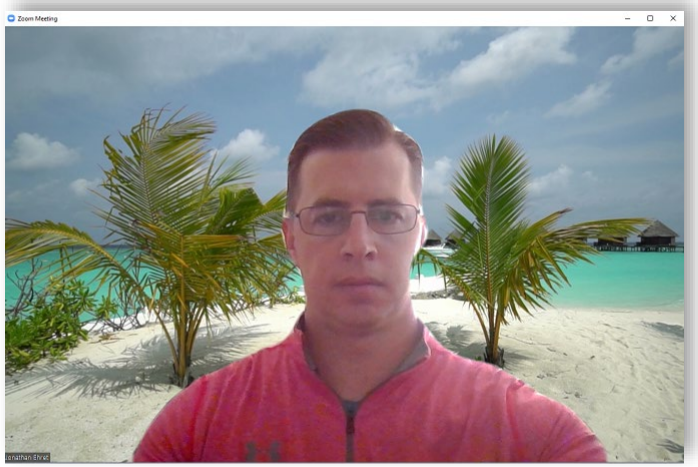


FIGURE 15: DO VENDORS MEET SECURITY REQUIREMENTS?

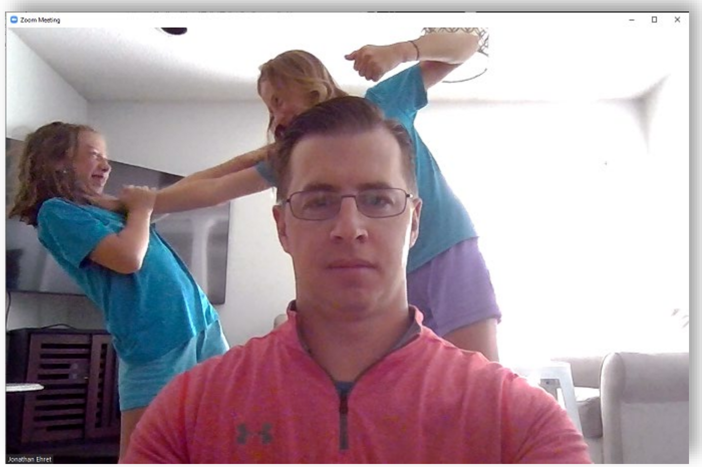


Let’s talk about questionnaires….

- Questionnaires are the most widely used TPRM tool
- Only offer a curated view of the controls in place
  - The vendor typically provides the evidence that makes them look good
  - Perception and reality are often very different



Perception



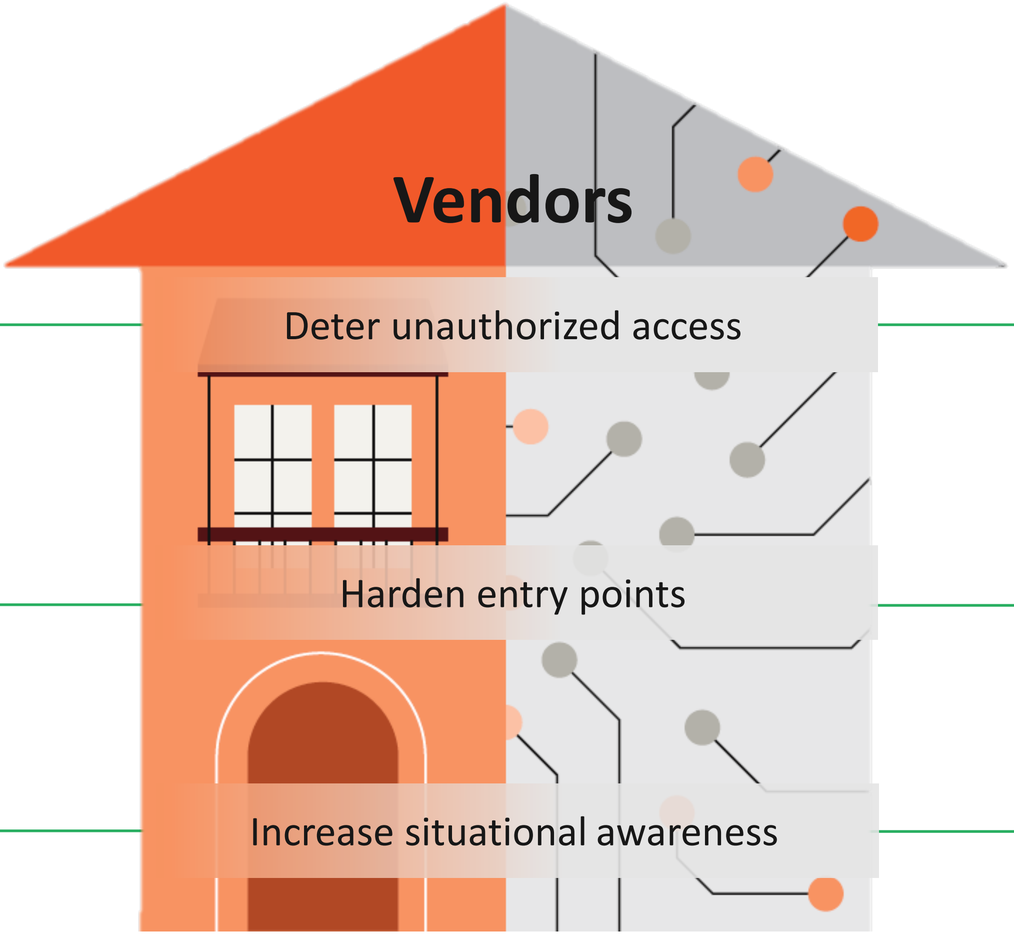
Reality

Some Questions

- Is my vendor really managing risk well, or are they just good at answering questionnaires? Will this vendor really protect my risk interests?
- What is my third-party risk exposure today? Is it getting better or worse?
- Where do I prioritize my resources to tackle third-party risk?

Continuous monitoring data (such as from RiskRecon) can help with this….

Continuous Monitoring: Sort of like the neighborhood watch



Vendors

Closed Windows, Fence, Flood Lights, Privacy Blinds

Deter unauthorized access

Patch Management

Deadbolt, Door Knob Locks, Locked Wi-Fi Network

Harden entry points

Web Security

Alarm System, Security Cameras

Increase situational awareness

Threat Intelligence

Researching risk factors at scale – RiskRecon & Cyentia

INTERNET RISK SURFACE REPORT

Exposure in a Hyper-Connected World

A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon Cyentia

CLOUD RISK SURFACE REPORT

Navigating safely in cloudy conditions

A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon Cyentia

RIPPLES ACROSS THE RISK SURFACE

A study of security incidents impacting multiple parties

A collaborative research project between RiskRecon and the Cy

riskrecon Cy

INTERNET RISK SURFACE IN THE FINANCIAL SECTOR

Benchmarking digital risk factors facing financial service firms

A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon mastercard Cyentia

riskrecon mastercard

33% of firms expose unsafe network services to the Internet

5x Firm exposing 9+ unsafe services have 5x higher rate of security findings

59% of servers running unsafe services also run behind in software patching

Analysis conducted by Cyentia Institute

Third-Party Security Signals

Exposing the reality of unsafe network services

A vast array of services form the underpinnings of enterprise network architectures that move and store data, enable administration of systems, and foster accessibility between entities. Though necessary in the era of digital transformation, such services arguably offer the most direct and tenuous pathways to an organization's critical assets. Attackers know this well and are quick to leverage unsafe network services to undermine a firm's cyber security posture.[1]

Though we colloquially dub data storage, network admin, and remote access services "unsafe," this is somewhat misleading, as their proper usage is not inherently dangerous. But when inadvertently or indiscriminately exposed to the internet, services like the ones above supply a seductive gateway for bad actors. A quick scan of a target's external infrastructure is all that's needed to reveal a not-so-secret entrance for opportunistic attackers. No sophistication or persistence needed.

Eliminating unsafe network services from your own infrastructure is challenging enough; ens
the same is on another
organizations in your thi
to the Internet. When you
performance, it's crucial

In this report, we'll exa
leveraging data from Ris
hosts and the services
hosts across 40,000 com
personal websites. Witho
what these organizations,
expose to the Internet for
look at whether these ser
issues across the network

This is a
between

[1] For example, automated attack
RDP and Microsoft SQL Server a
online by scanning for exposed

WEAVING A SAFER WEB

riskrecon mastercard

22% of firms have not fully implemented TLS 1.2

70% higher security findings in firms that don't fully support TLS 1.2

67% of servers running older TLS versions also struggle to patch software

Analysis conducted by Cyentia Institute

Weaving a Safer Web

The State & Significance of TLS 1.2 Support

Communicating securely on the web is fundamental to the operation of the Internet. Various TLS (previously SSL) protocols deploy an apparatus of interlocking cryptographic algorithms, kept in check by a widespread network of certificate authorities to ensure the little green lock at the top of our browser helps us feel safe.

Because TLS is the conduit through which a great deal of juicy personal and financial information flows on the internet, it has long been a target of security researchers. These whitehat crypto-nerds have uncovered a menagerie of sinister-sounding vulnerabilities across multiple TLS versions, which are often decried as harbingers of Armageddon on the Internet. Perhaps this is why TLS exploits have long held the crown for "protocol most likely to have a branded vulnerability."

All this protocol breaking and refining has brought us to the current state of the affairs wherein the Internet Engineering Task Force, the National Institute for Standards and Technology, and the Payment Card Industry Security Standards Council are mandating that operators of web servers migrate to using TLS 1.2 in 2020. Additionally, TLS 1.0 and 1.1 have been (or are in the process of being) deprecated in one way or another by major browsers. This means visitors will have to navigate around cryptic browser warnings in the very near future if your website doesn't support TLS 1.2. Definitely not a good look.

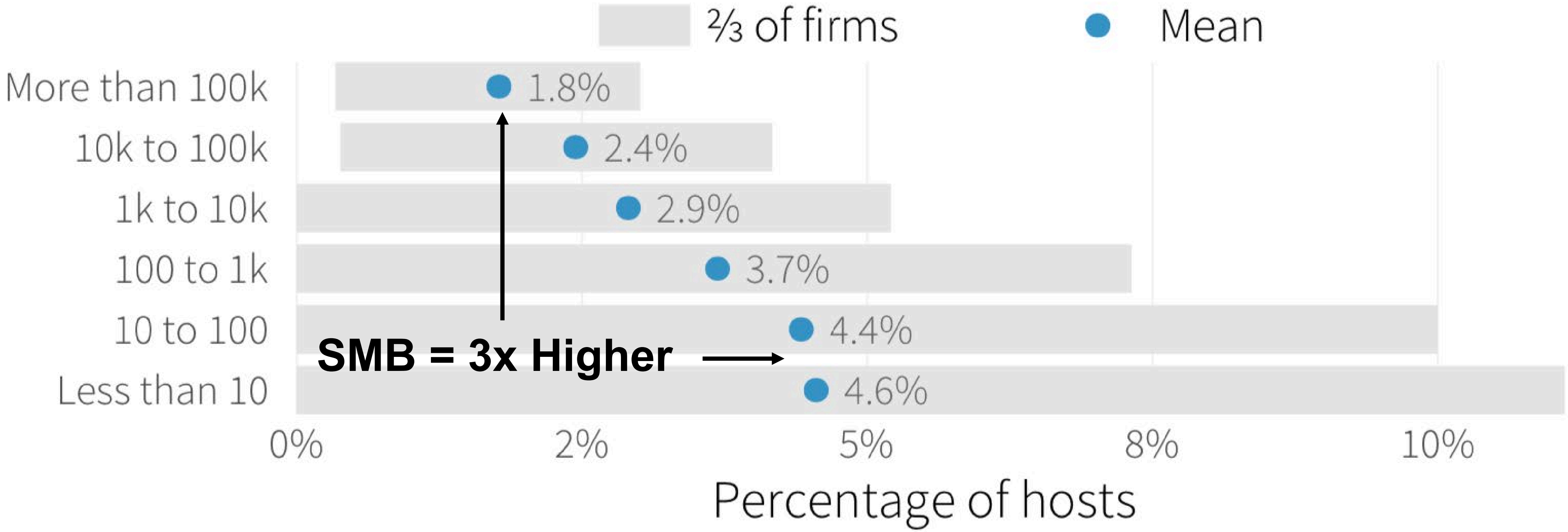
In this report, we'll zoom in on the state of TLS 1.2 implementation across the Internet. We'll leverage RiskRecon's unique scan data on millions of web servers around the world to see where the rollout of TLS 1.2 is going smoothly and where it is meeting resistance. Additionally, we'll show that not supporting TLS 1.2 isn't just bad for the customers visiting unsupported websites, but can be an indicator of other security problems within an organization.

> The big takeaway is that if firms can't implement TLS 1.2 comprehensively, then they likely have bigger security holes in their network.

[2] POODLE, BEAST, Logjam, DROWN, FREAK…hackers love getting creative with their acronyms.

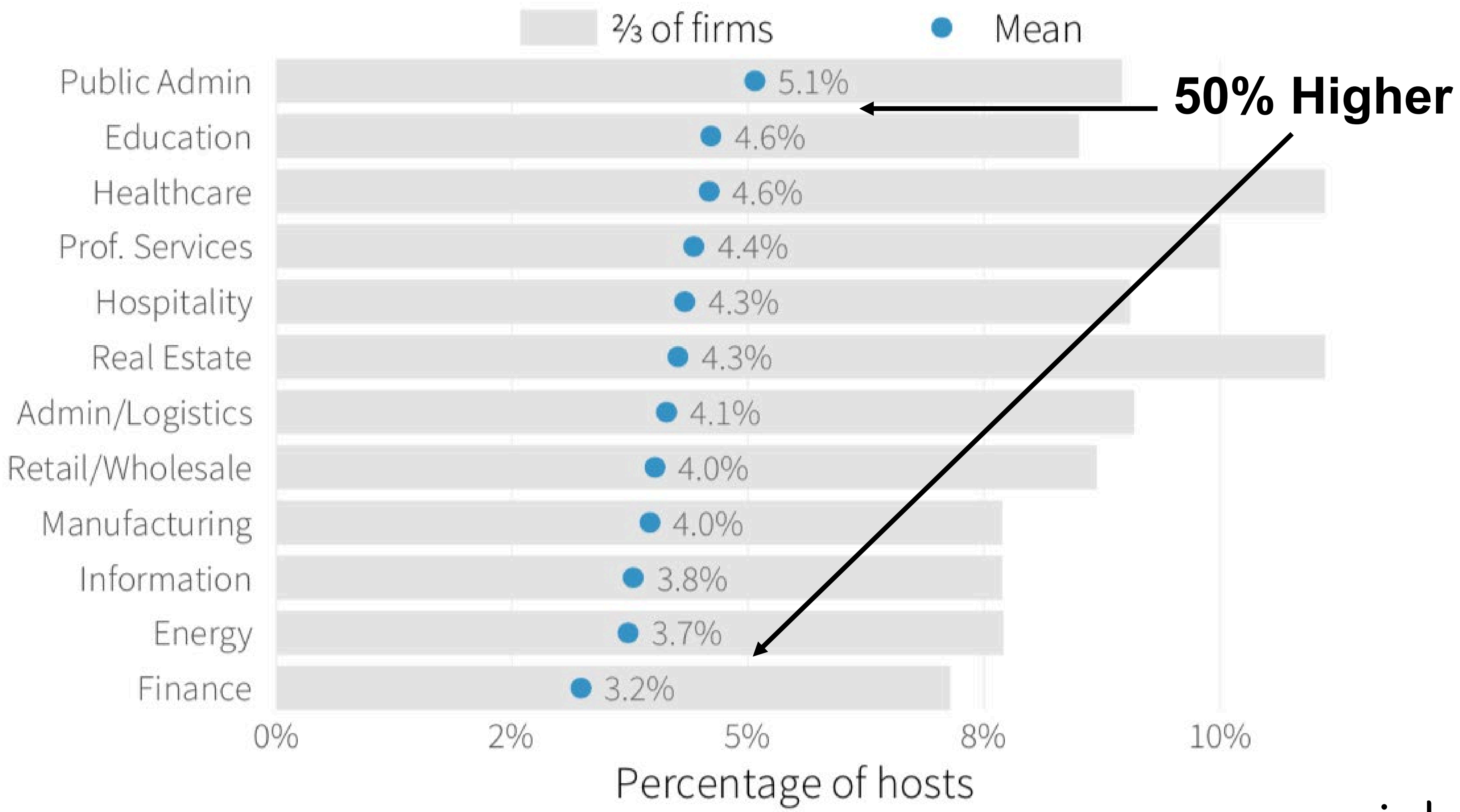
WEAVING A SAFER WEB RISKRECON.COM | 1

FIGURE 18: Hosts with high or critical findings by organization size



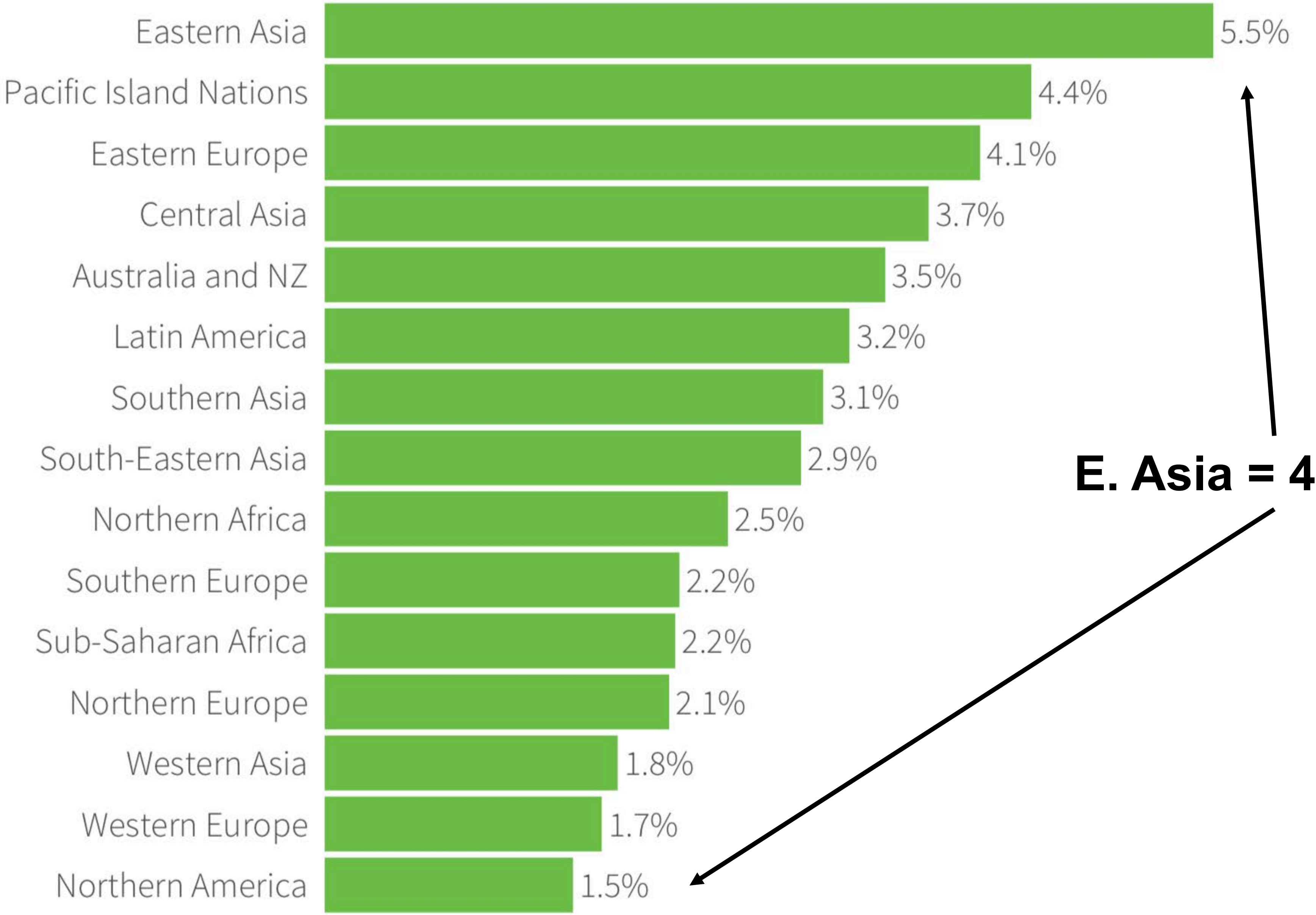
SMB = 3x Higher

FIGURE 17: Hosts with high or critical findings by industry



50% Higher

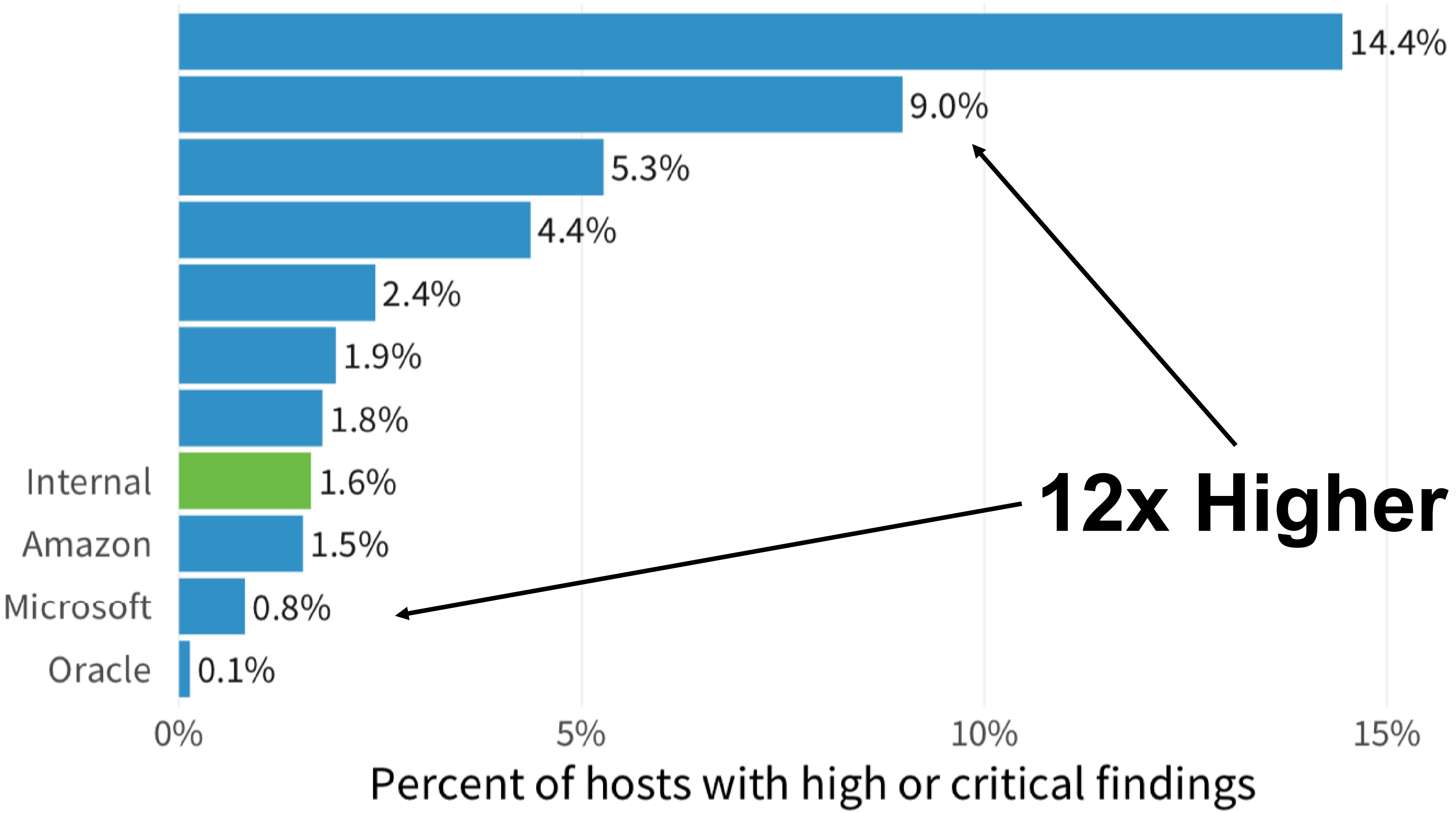
FIGURE 19: Percentage of hosts with high or critical findings



E. Asia = 4x Higher

riskrecon
mastercard

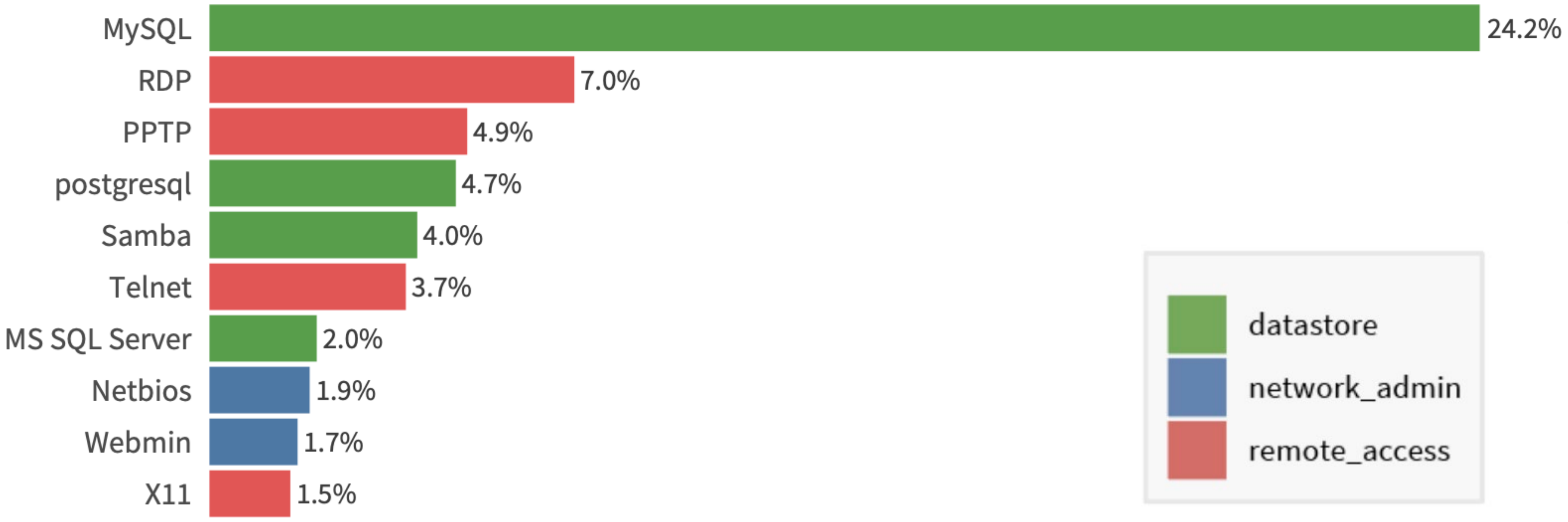
Figure 16: Percent of hosts with high or critical findings in top clouds



12x Higher

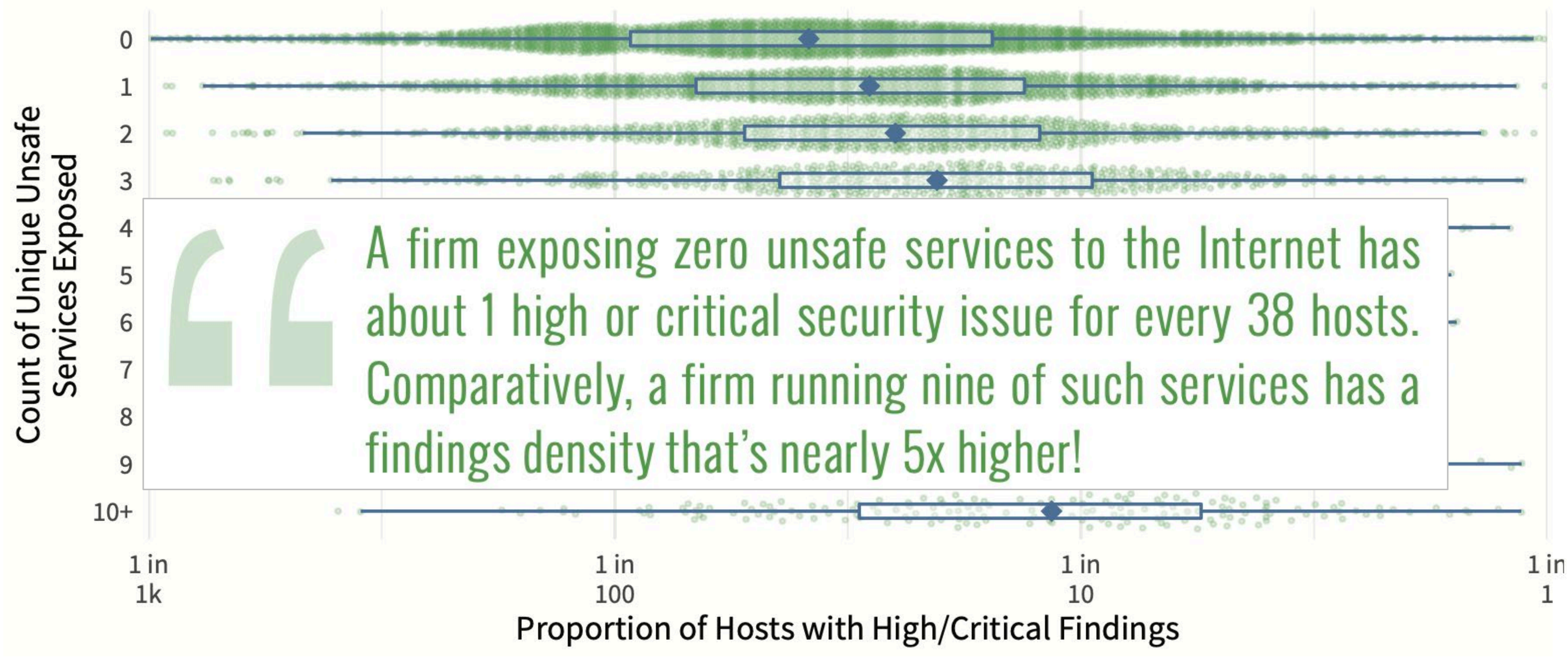
Unsafe services as an indicator of broader security issues

FIGURE 3: PREVALENCE OF UNSAFE SERVICES CATEGORIES EXPOSED BY FIRMS



Unsafe services as an indicator of broader security issues

FIGURE 7: PROPORTION OF FIRMS EXPOSING MULTIPLE UNSAFE SERVICES

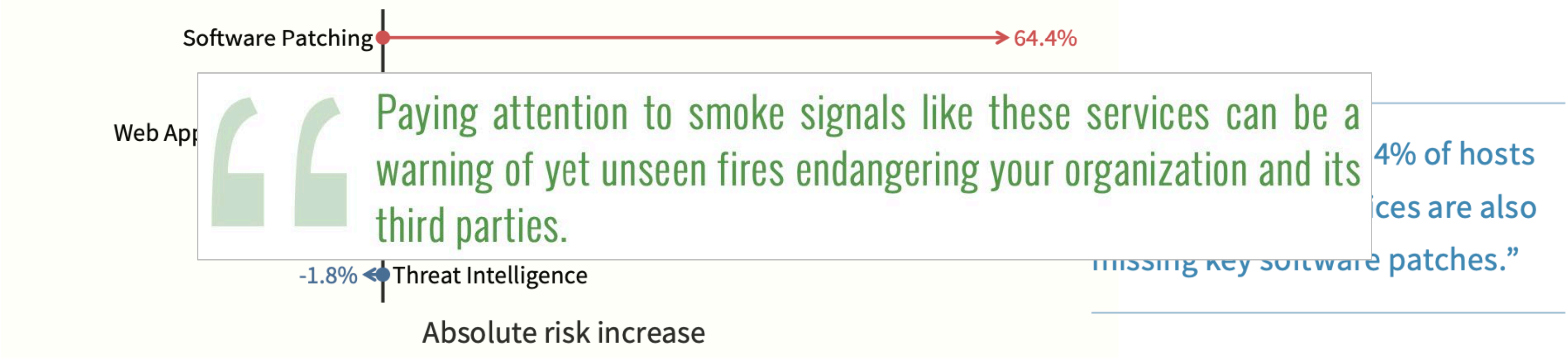


> A firm exposing zero unsafe services to the Internet has about 1 high or critical security issue for every 38 hosts. Comparatively, a firm running nine of such services has a findings density that's nearly 5x higher!

The green dots in Figure 7 show the percent of each firm's external hosts that exhibit high or critical security findings. The blue dots mark the average for each group, making it clear that the rate of severe security problems increases consistently with the number of unsafe services.

Unsafe services as an indicator of broader security issues

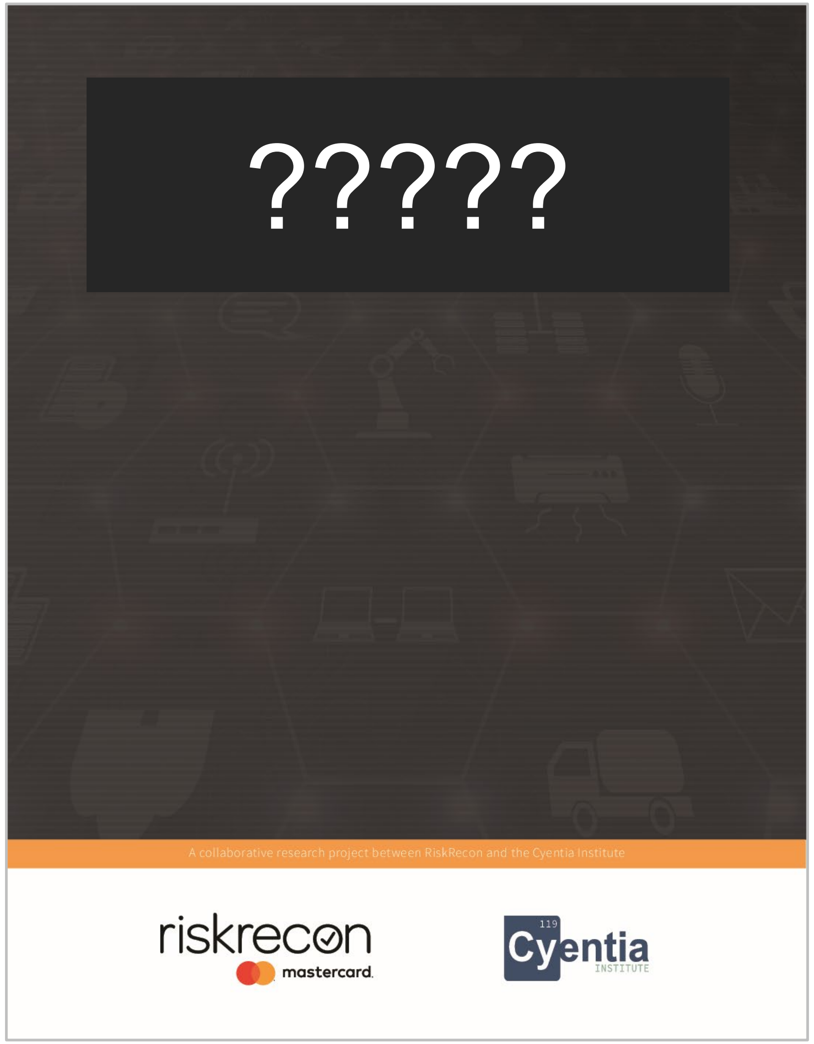
FIGURE 9: TYPES OF FINDINGS CORRELATED WITH EXPOSURE OF UNSAFE SERVICES



4% of hosts … ices are also missing key software patches.”

> Paying attention to smoke signals like these services can be a warning of yet unseen fires endangering your organization and its third parties.

Sneak peak: Untitled, Unpublished Report



?????

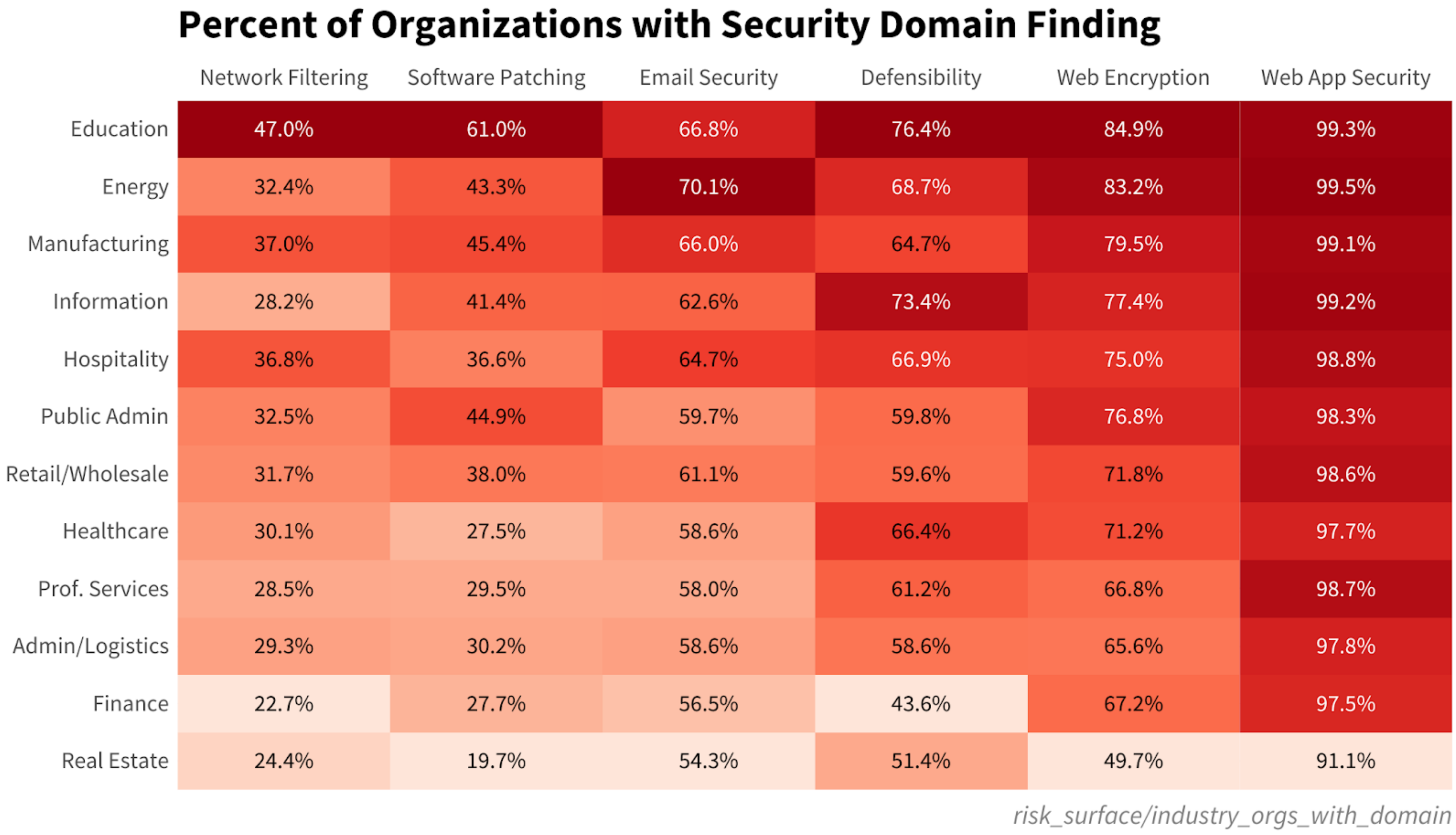
A collaborative research project between RiskRecon and the Cyentia Institute

riskrecon mastercard

Cyentia Institute

- What can we infer about a vendor’s risk posture based on different levels of information?
- Can we build a model for predicting risk posture?
- Which factors provide the strongest predictive value?

Security findings by sector



Percent of Organizations with Security Domain Finding

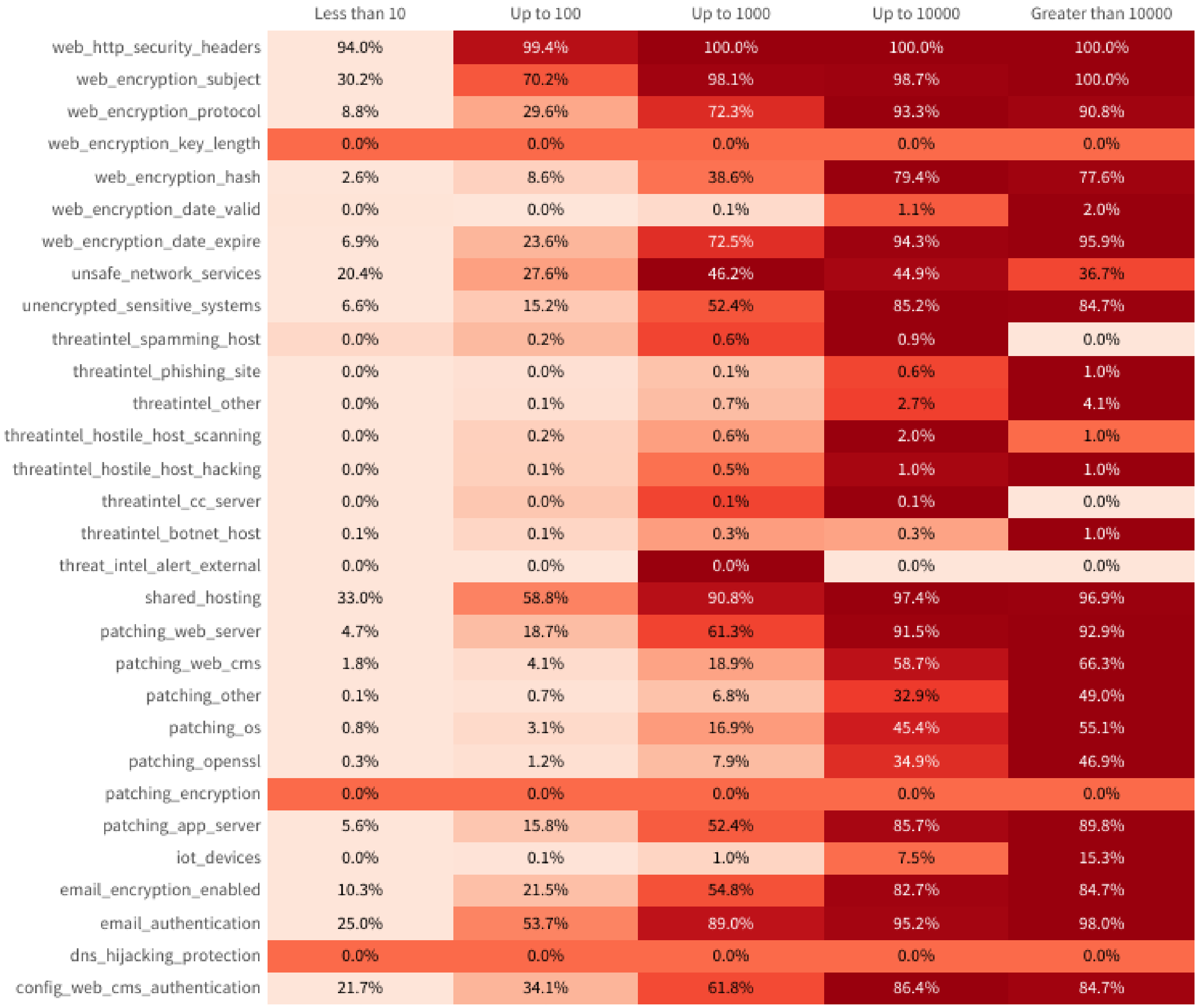
	Network Filtering	Software Patching	Email Security	Defensibility	Web Encryption	Web App Security
Education	47.0%	61.0%	66.8%	76.4%	84.9%	99.3%
Energy	32.4%	43.3%	70.1%	68.7%	83.2%	99.5%
Manufacturing	37.0%	45.4%	66.0%	64.7%	79.5%	99.1%
Information	28.2%	41.4%	62.6%	73.4%	77.4%	99.2%
Hospitality	36.8%	36.6%	64.7%	66.9%	75.0%	98.8%
Public Admin	32.5%	44.9%	59.7%	59.8%	76.8%	98.3%
Retail/Wholesale	31.7%	38.0%	61.1%	59.6%	71.8%	98.6%
Healthcare	30.1%	27.5%	58.6%	66.4%	71.2%	97.7%
Prof. Services	28.5%	29.5%	58.0%	61.2%	66.8%	98.7%
Admin/Logistics	29.3%	30.2%	58.6%	58.6%	65.6%	97.8%
Finance	22.7%	27.7%	56.5%	43.6%	67.2%	97.5%
Real Estate	24.4%	19.7%	54.3%	51.4%	49.7%	91.1%

risk_surface/industry_orgs_with_domain

Security findings by organization size

Percent of Organization Sizes with Finding Criteria

Fill by relative concentration across criteria



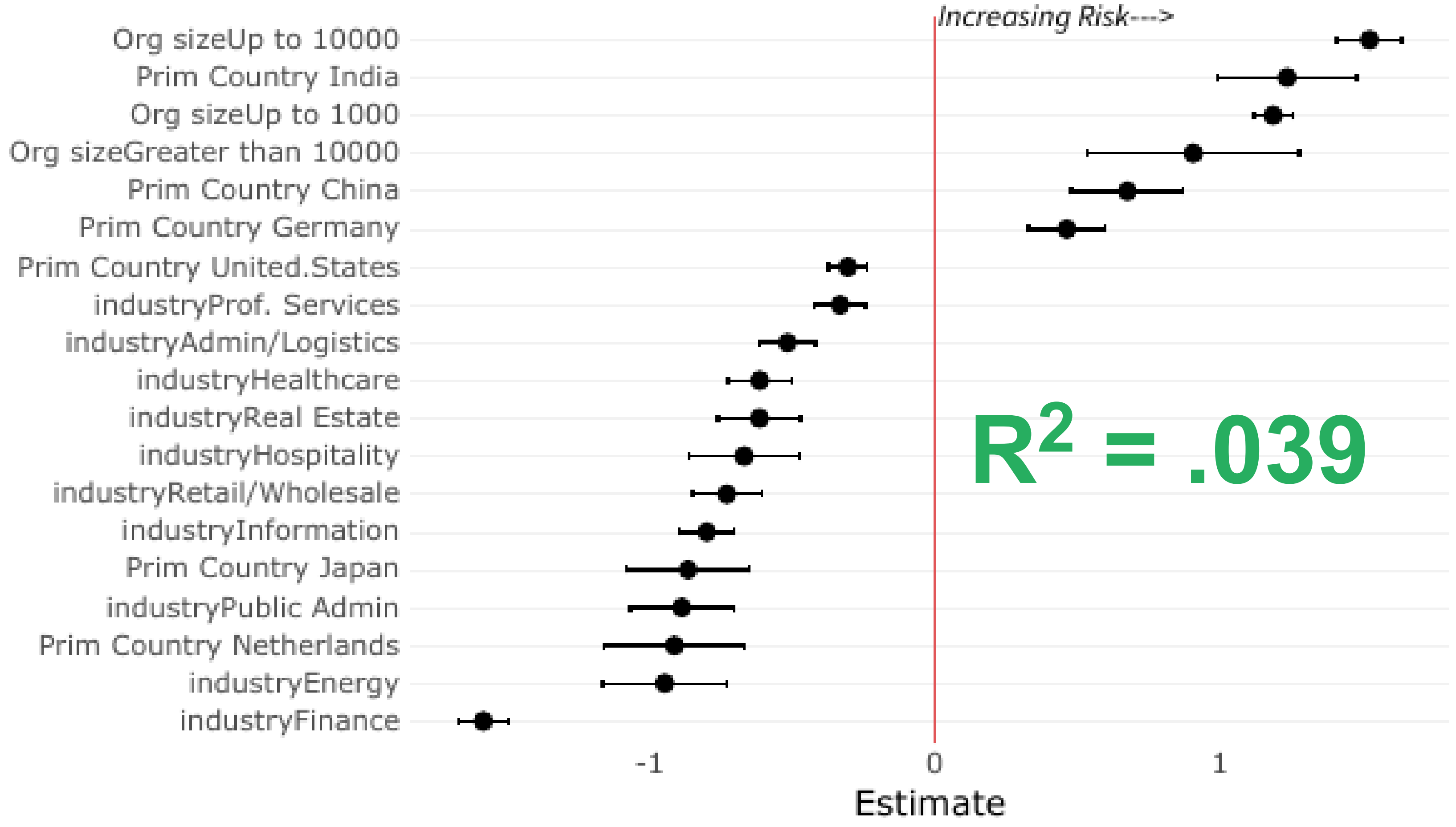
	Less than 10	Up to 100	Up to 1000	Up to 10000	Greater than 10000
web_http_security_headers	94.0%	99.4%	100.0%	100.0%	100.0%
web_encryption_subject	30.2%	70.2%	98.1%	98.7%	100.0%
web_encryption_protocol	8.8%	29.6%	72.3%	93.3%	90.8%
web_encryption_key_length	0.0%	0.0%	0.0%	0.0%	0.0%
web_encryption_hash	2.6%	8.6%	38.6%	79.4%	77.6%
web_encryption_date_valid	0.0%	0.0%	0.1%	1.1%	2.0%
web_encryption_date_expire	6.9%	23.6%	72.5%	94.3%	95.9%
unsafe_network_services	20.4%	27.6%	46.2%	44.9%	36.7%
unencrypted_sensitive_systems	6.6%	15.2%	52.4%	85.2%	84.7%
threatintel_spamming_host	0.0%	0.2%	0.6%	0.9%	0.0%
threatintel_phishing_site	0.0%	0.0%	0.1%	0.6%	1.0%
threatintel_other	0.0%	0.1%	0.7%	2.7%	4.1%
threatintel_hostile_host_scanning	0.0%	0.2%	0.6%	2.0%	1.0%
threatintel_hostile_host_hacking	0.0%	0.1%	0.5%	1.0%	1.0%
threatintel_cc_server	0.0%	0.0%	0.1%	0.1%	0.0%
threatintel_botnet_host	0.1%	0.1%	0.3%	0.3%	1.0%
threat_intel_alert_external	0.0%	0.0%	0.0%	0.0%	0.0%
shared_hosting	33.0%	58.8%	90.8%	97.4%	96.9%
patching_web_server	4.7%	18.7%	61.3%	91.5%	92.9%
patching_web_cms	1.8%	4.1%	18.9%	58.7%	66.3%
patching_other	0.1%	0.7%	6.8%	32.9%	49.0%
patching_os	0.8%	3.1%	16.9%	45.4%	55.1%
patching_openssl	0.3%	1.2%	7.9%	34.9%	46.9%
patching_encryption	0.0%	0.0%	0.0%	0.0%	0.0%
patching_app_server	5.6%	15.8%	52.4%	85.7%	89.8%
iot_devices	0.0%	0.1%	1.0%	7.5%	15.3%
email_encryption_enabled	10.3%	21.5%	54.8%	82.7%	84.7%
email_authentication	25.0%	53.7%	89.0%	95.2%	98.0%
dns_hijacking_protection	0.0%	0.0%	0.0%	0.0%	0.0%
config_web_cms_authentication	21.7%	34.1%	61.8%	86.4%	84.7%

risk_surface/sec_crit_org_size

Firmographics-only model

Significant Estimators for Flaw Density

(High Value Asset & High Sev Findings) ~ Business Factors



R^2 = .039

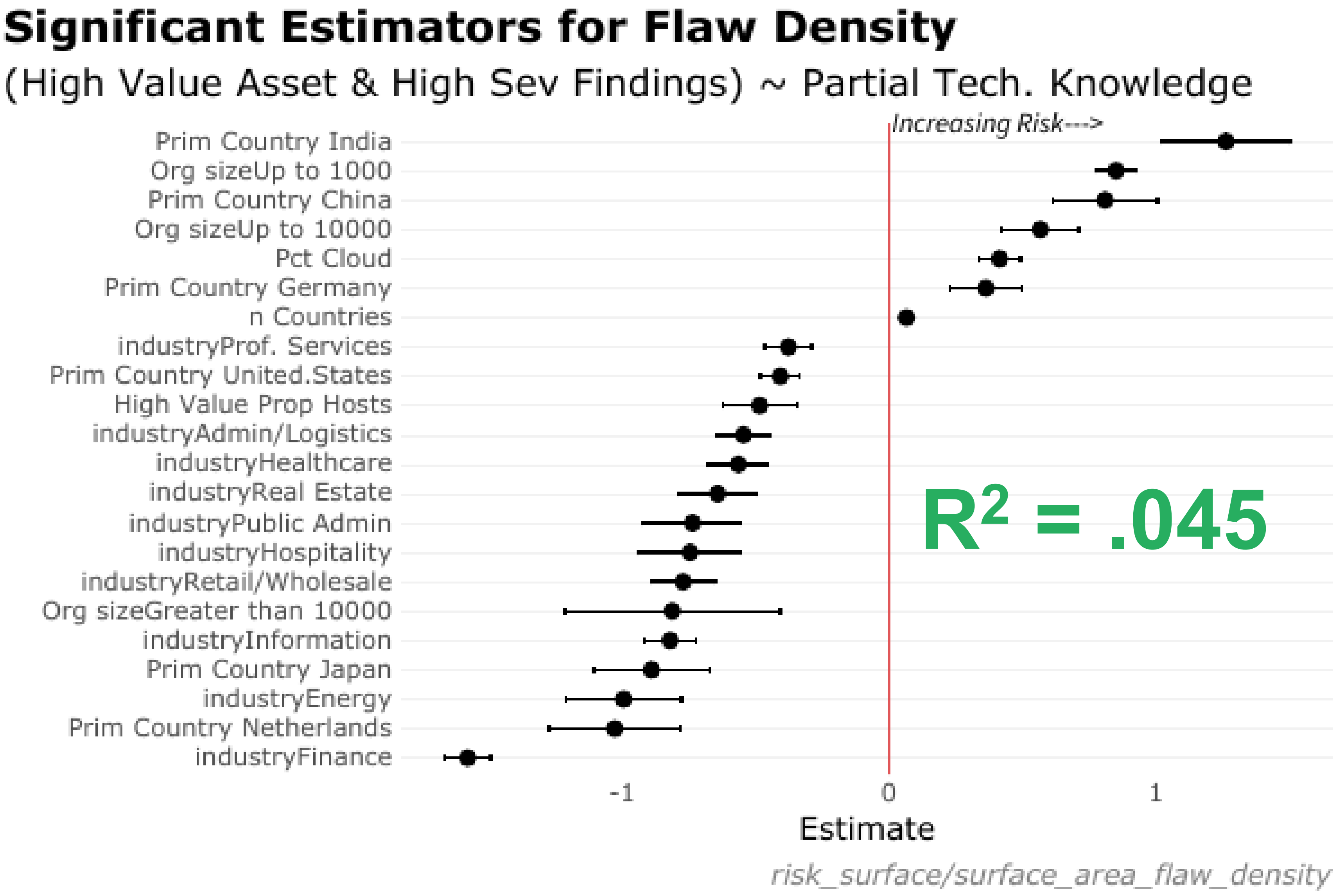
risk_surface/business_parameters_flaw_density

Features - Minimal Information

variable	type	role
finding_density	numeric	outcome
prim_country	nominal	predictor
industry	nominal	predictor
org_size	nominal	predictor

features_minimal_info

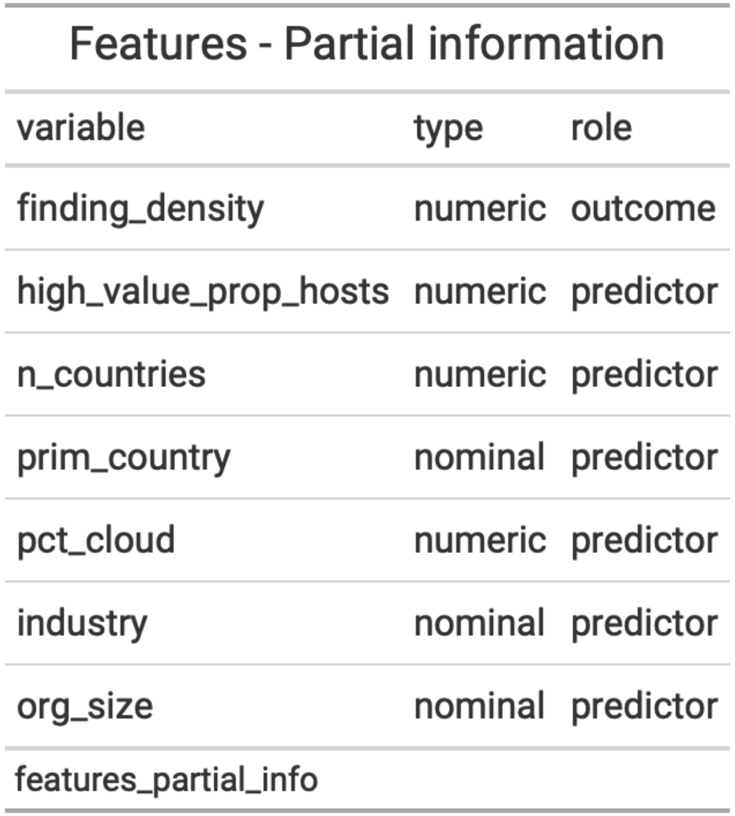
Infrastructure-based model



Significant Estimators for Flaw Density

(High Value Asset & High Sev Findings) ~ Partial Tech. Knowledge

$R^2 = .045$



Features - Partial information

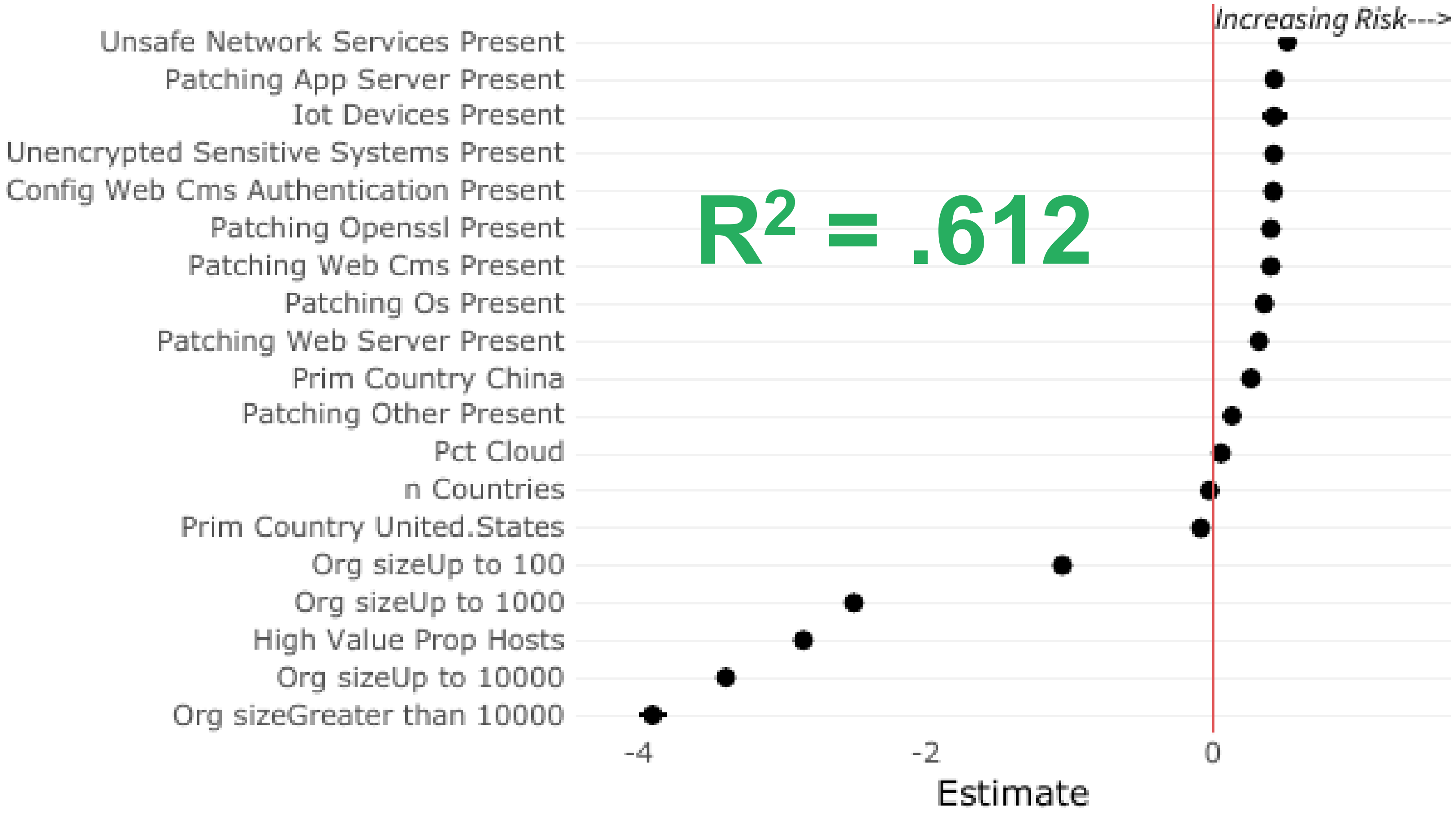
variable	type	role
finding_density	numeric	outcome
high_value_prop_hosts	numeric	predictor
n_countries	numeric	predictor
prim_country	nominal	predictor
pct_cloud	numeric	predictor
industry	nominal	predictor
org_size	nominal	predictor

features_partial_info

Assessment-based model

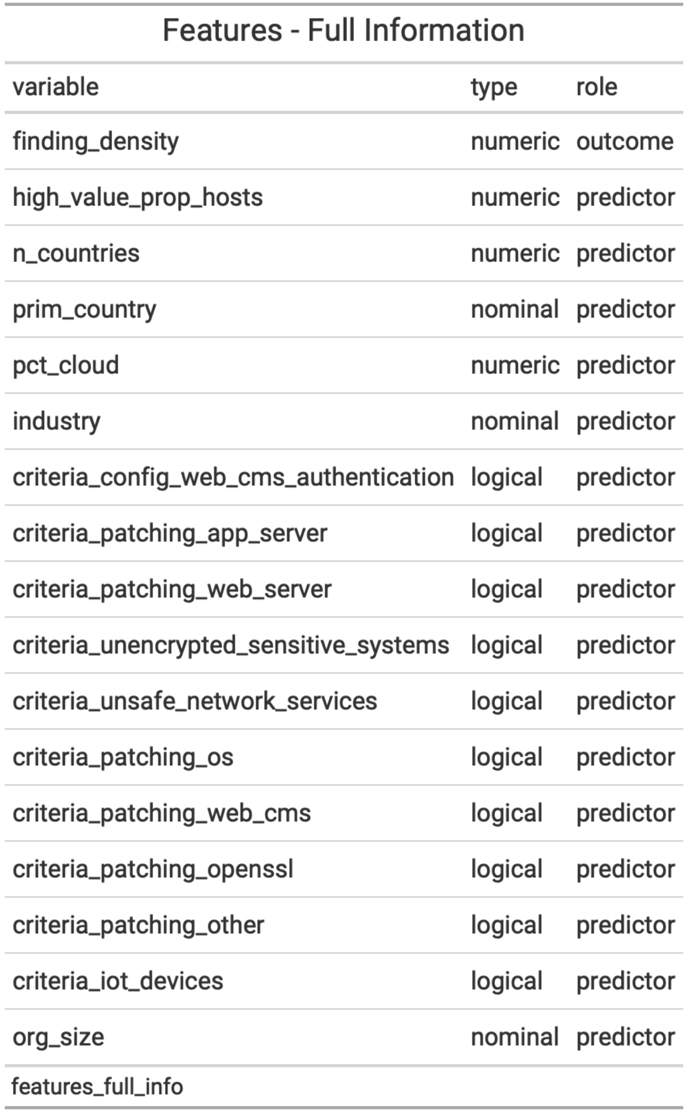
Significant Estimators for Flaw Density

(High Value Asset & High Sev Findings) ~ Full Technical Information



$R^2 = .612$

risk_surface/parameters_flaw_density

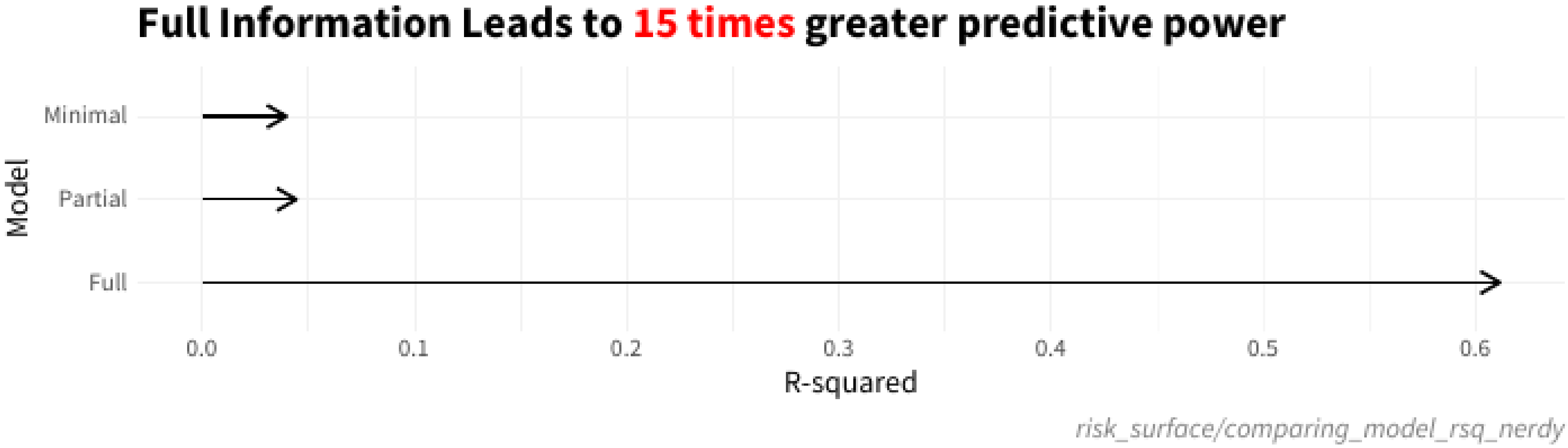


Features - Full Information

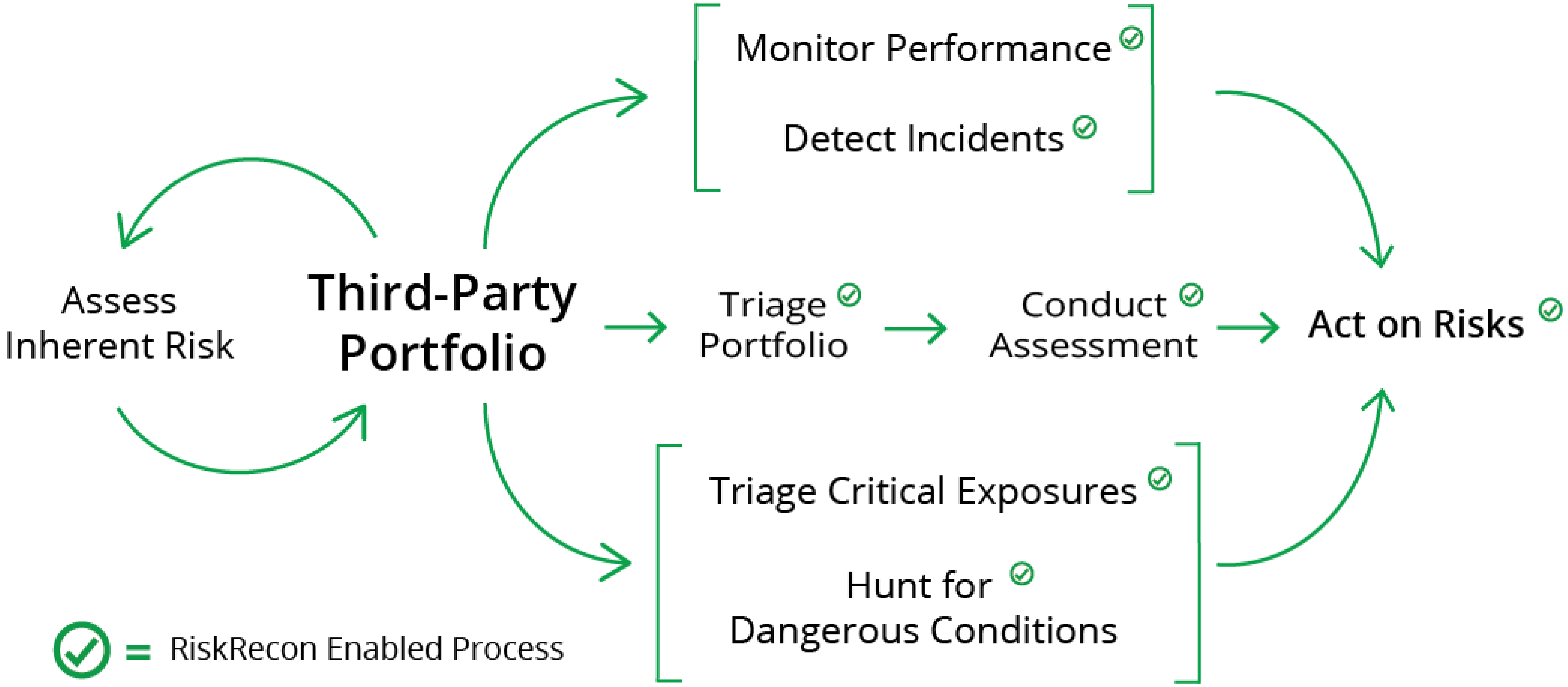
variable	type	role
finding_density	numeric	outcome
high_value_prop_hosts	numeric	predictor
n_countries	numeric	predictor
prim_country	nominal	predictor
pct_cloud	numeric	predictor
industry	nominal	predictor
criteria_config_web_cms_authentication	logical	predictor
criteria_patching_app_server	logical	predictor
criteria_patching_web_server	logical	predictor
criteria_unencrypted_sensitive_systems	logical	predictor
criteria_unsafe_network_services	logical	predictor
criteria_patching_os	logical	predictor
criteria_patching_web_cms	logical	predictor
criteria_patching_openssl	logical	predictor
criteria_patching_other	logical	predictor
criteria_iot_devices	logical	predictor
org_size	nominal	predictor

features_full_info

From Uncertainty to Understanding



Third-Party SecOps Framework



✓ = RiskRecon Enabled Process

Thank you.