



# The Supply Chain Minority Report:

Heading Off Breaches and Ransomware  
Events Before They Impact Operations

Jonathan Ehret  
*Vice President, Customer Enablement*  
*RiskRecon, a Mastercard Company*





## About the Speaker



Jon Ehret is Vice President of Customer Enablement for RiskRecon, a Mastercard company. Jon brings 20+ years of experience in technology and risk, including extensive experience building, maturing and running third party risk programs in both the finance and healthcare industries.

Before joining RiskRecon, Jon built and lead the third-party risk program for BlueCross BlueShield of WNY and also served as President and Co-founder of the Third Party Risk Association, an international professional association of third party risk practitioners and vendors.

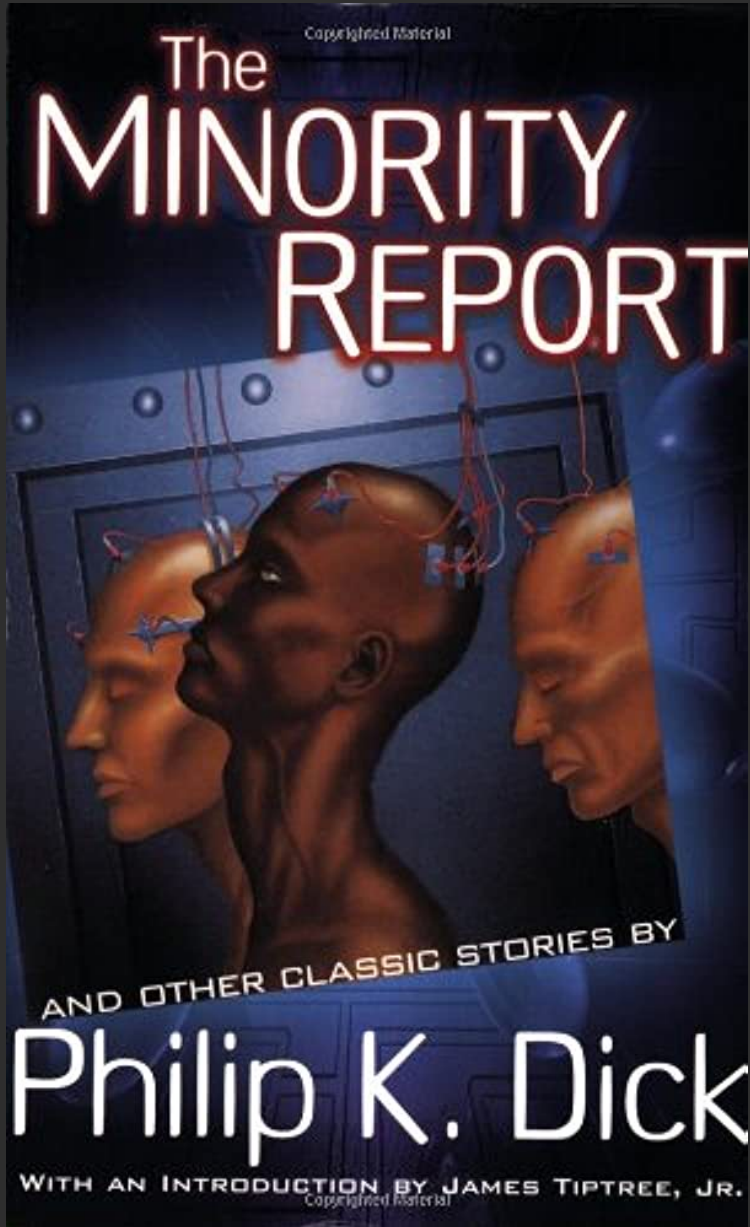
# Agenda



- What is The Minority Report?
- Lessons learned from analyzing breach and ransomware events
- How can we attempt to predict where breaches and ransomware will impact our supply chain



# What is The Minority Report?



- Classic Science Fiction novel written by Philip K. Dick
  - Made into a Hollywood movie starring Tom Cruise
- Premise:
  - Crime in the future is fought before it happens. "Precogs", mutants with the ability to see the future, are utilized by the PreCrime division to identify people who will commit crimes in the future. The police arrest these individuals before they actually commit any crime.
- A bit of a scary real world premise and purely science fiction.....but what if we could move in this direction to secure our supply chain??
- Let's look at some data.....



# What Data Did We Look At?



- Risk Insights from 10 Years of Breach Event Monitoring of 109,000 Companies
  - <https://www.riskrecon.com/paper-risk-management-insights-from-10-years-of-data-breach-events>
- Five Lessons From 1,000 Destructive Ransomware Events
  - <https://www.riskrecon.com/report-five-lessons-learned-from-ransomware-attacks>



# Data Source: RiskRecon Cybersecurity Assessment Platform

**Udrane galactic university** | Assessment Date: Feb 2, 2022

**RiskRecon Rating:** F (3.7/10)

**Industry Ratings:** 6.2 Industry Average, 3rd Percentile Rank

Domain	Rating	Trend	Domain	Rating	Trend
Software Patching	D 4.5	0.0	System Reputation	F 3.7	+0.1
Application Security	F 2.6	0.0	Email Security	D 5.3	0.0
Web Encryption	B 8.3	+0.1	DNS Security	F 3.8	0.0
Network Filtering	F 0.0	0.0	System Hosting	D 5.1	0.0
Preach Events	C 5.6	0.0			

**Action Plan Status:** 1,676 Current Open Issues, 1,640 Current Shared Issues, 11,850 Total Resolved Issues, 13,490 Total Shared Issues, 04/08/2020 Issues Last Shared

**Risk Priority Matrix:** High (1K, 326, 436, 120 issues), Medium (962, 763, 250, 113 issues)

**Critical Severity Issues in High Value Assets:**

Security Criteria	Issue	Asset	Hostname
Application Server Patching	PHP 5.3.x	354.7382.4.185	www.mis...
Application Server Patching	PHP 5.3.x	354.7382.3.11	friend.weblog...
Application Server Patching	PHP 5.3.x	354.7382.395.115	pub.udrane.edu
Application Server Patching	PHP 5.4.x	354.801.10.65	galaxyletters...
Application Server Patching	PHP 5.3.x	354.7382.243.19	udrane.farthing.org

**Software Patching** | Base Weight: 30%

Rating: D (4.4/10)

Security Criteria	Rating	Issue Count
Application Server Patching	F 1.8	76
OpenGL Patching	F 1.8	1
OpenSSL Patching	F 1.8	14
Web Server Patching	C 5.1	16

**Application Security** | Base Weight: 12.5%

Rating: F (2.4/10)

Security Criteria	Rating	Issue Count
CMS Authentication	F 0.0	515
HTTP Security Headers	C 5.2	1,399
Control Threat Intelligence Alerts	Info	2
High Level System Encryption	Info	15
Webinar Code	Info	0

**Web Encryption** | Base Weight: 12.5%

Rating: B (6.1/10)

Security Criteria	Rating	Issue Count
Certificate Expiration Date	C 6.8	1,122
Certificate Valid Date	A 16	0
Encryptor Mail Algorithms	A 5.2	10
Encryptor Key Length	A 16	0
Encryptor Protocols	A 5.2	0
Certificate Subject	C 5.2	206

**Network Filtering** | Base Weight: 10%

Rating: F (0.0/10)

Security Criteria	Rating	Issue Count
Linux Kernel/Kernel	F 0.0	1,017
IoT Devices	A 16	0

**Breach Events** | Base Weight: 10%

Rating: D (5.1/10)

Security Criteria	Rating	Issue Count
Preach Event: 0 - 6 Months	A 16	0
Preach Event: 6 - 12 Months	A 16	0
Preach Event: 12 - 24 Months	C 4.0	1

**Software Patching** | Base Weight: 30%

Rating: D (4.5/10)

**Summary Metrics:** 1,451 Observations, 132 Issue Count, 9% Issue Rate

**Industry Rating:** 6.8 Industry Avg, 19th Percentile Rank

Security Criteria	Rating	Issue Count	Population	Issue Rate
Application Server Patching	F 1.8	69	202	26%
OpenGL Patching	B 7.9	3	89	3%
CMS Patching	B 7.9	5	170	3%
Web Server Patching	C 6.0	55	921	6%

**Table of Open Issues:**

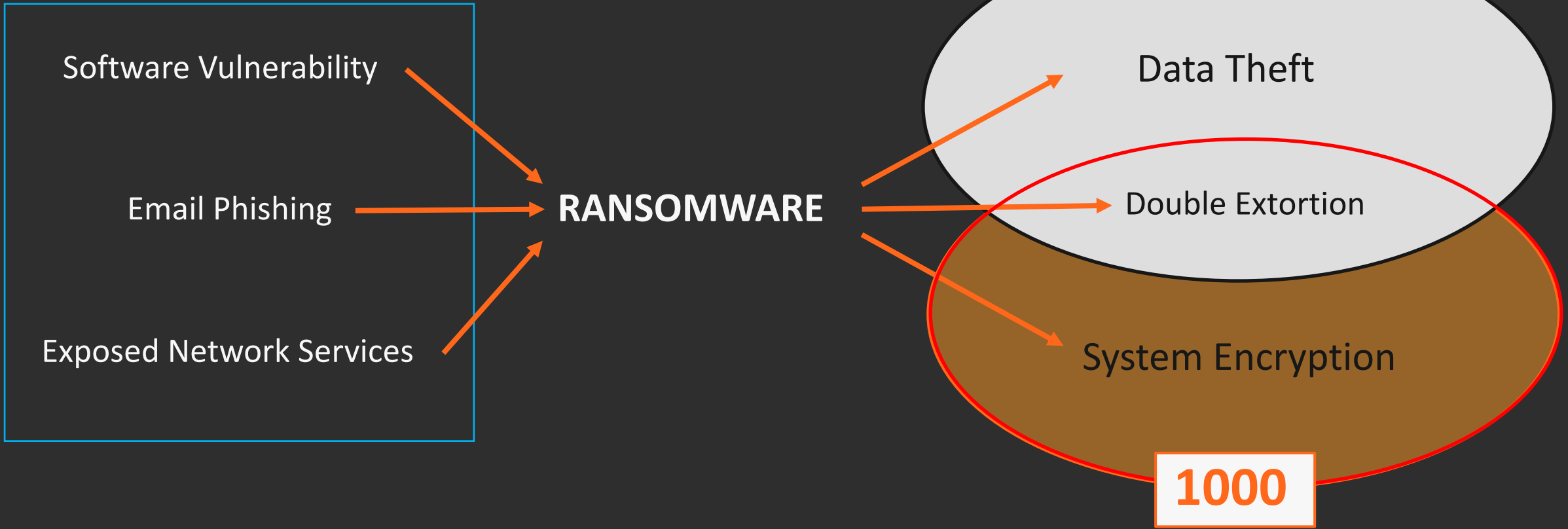
Software	IP Address	Hostname	Days Open	Asset Value	Severity	Priority	Action Plan
Apache 2.2.x	354.7382.243.10	classic.molveneaaccess.udrane.edu	448	medium	medium	4	No
Apache 2.2.x	354.7382.4.185	www.udranepapers.info	412	medium	medium	4	No
Apache 2.2.x	354.797.1333.143	cs.udrane.edu	1351	medium	medium	4	No
Apache 2.2.x	377.220.3399.8	udranesocial.com	77	low	medium	5	No
Apache 2.2.x	377.220.3399.8	www.udranesocial.com	77	low	medium	5	No
Apache 2.2.x	377.220.3399.8	mail.udranesocial.com	77	low	medium	5	No
IS 6.0	308.86.251.2	stardust.org	1338	low	critical	3	Yes
IS 6.0	308.86.251.2	www.stardust.org	936	low	critical	3	Yes

Assessing and Rating ~15M Entities Worldwide



Publicly-Disclosed Events  
January 2016 – March 2022

>90% of initial  
compromise vectors



# RiskRecon Breach Study



- Sample Size: 109,000 companies
- Breaches Reviewed: 8,892
- Range: Jan 2012 – Dec 2021
- Publicly Disclosed Events Only



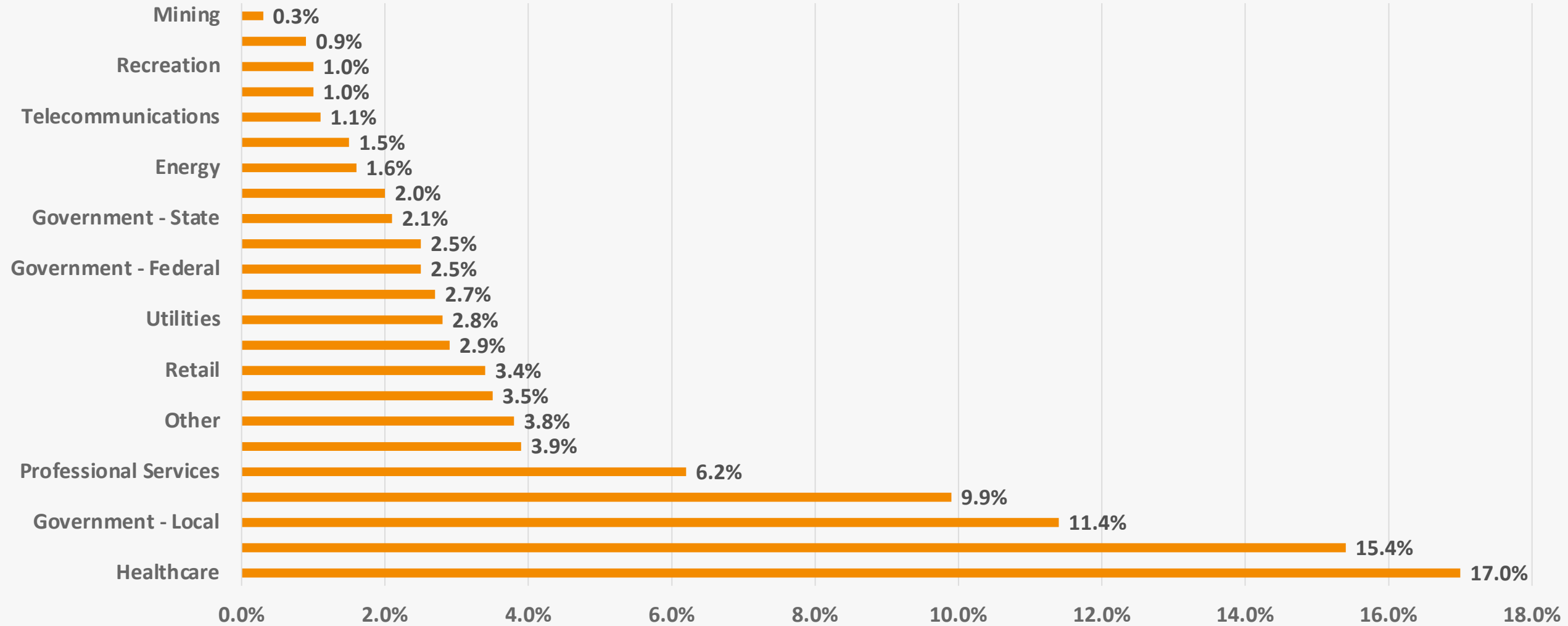


# Everyone is a Target



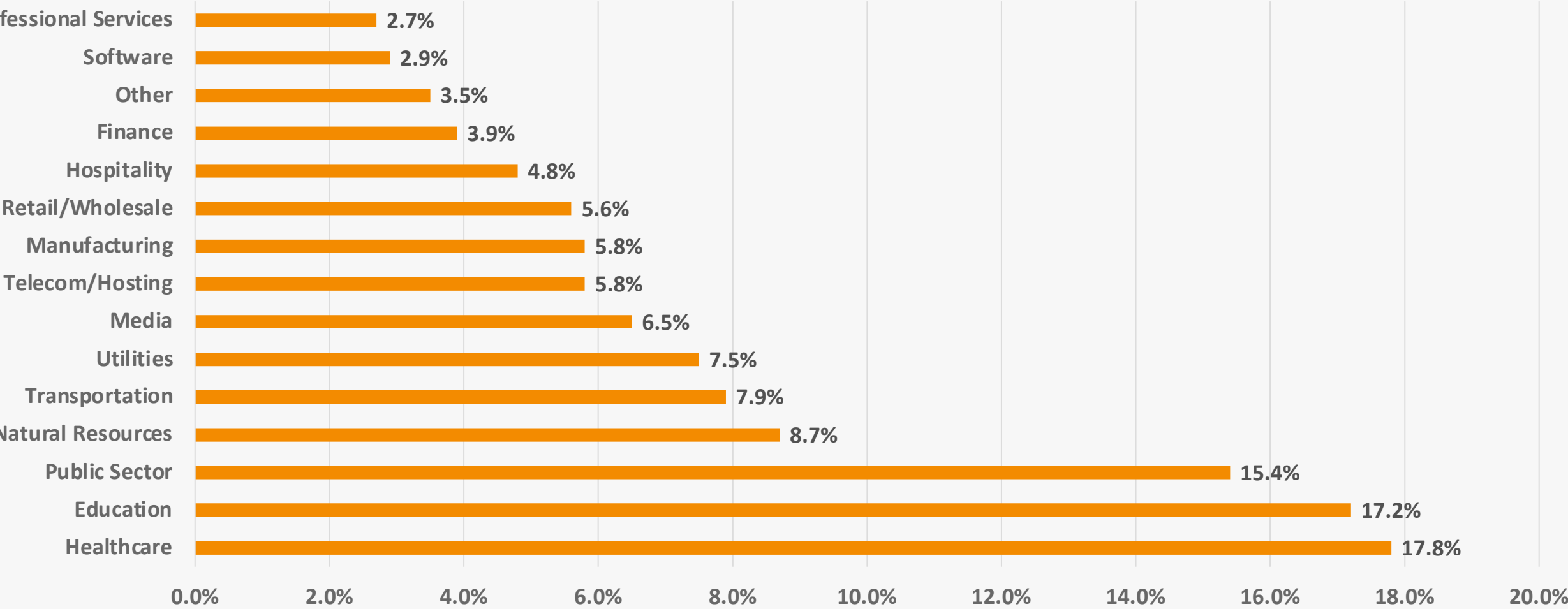
# Everyone is a Target

## Distribution of Destructive Ransomware Events by Industry Sector



# Everyone is a Target

Percent of Companies Publicly Reporting Breach by Industry 2012 - 2021

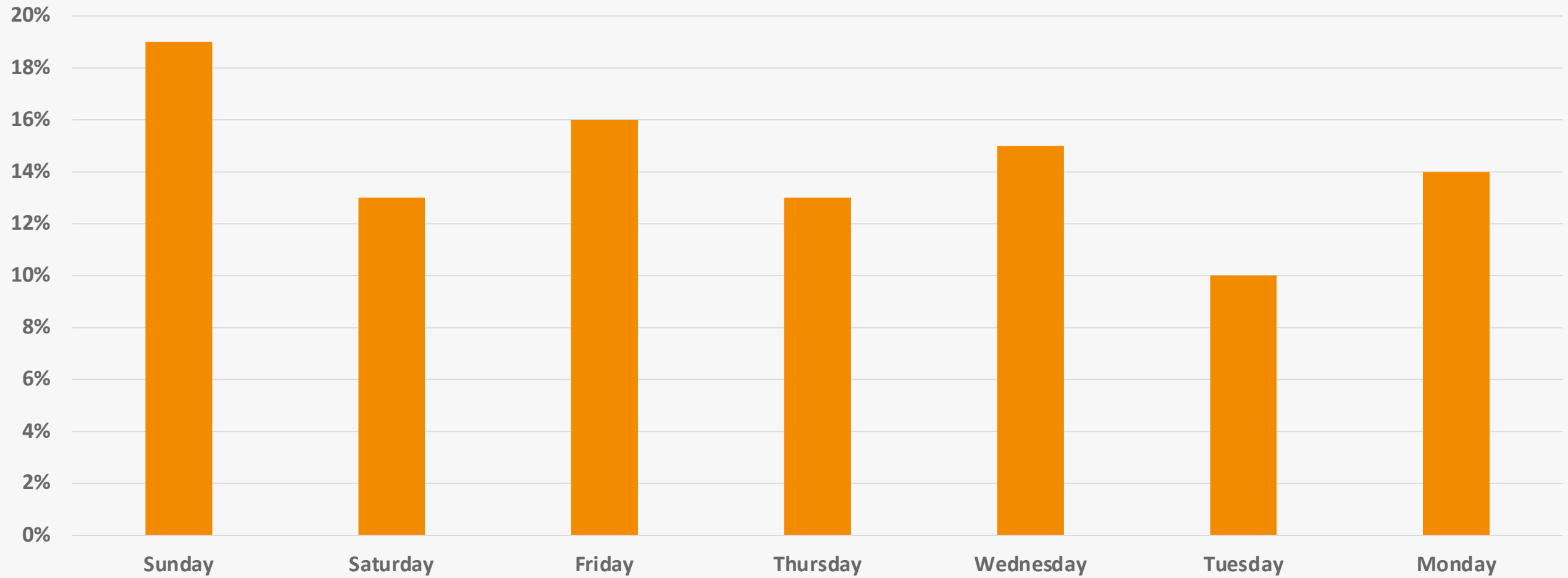


# No Day is Sacred



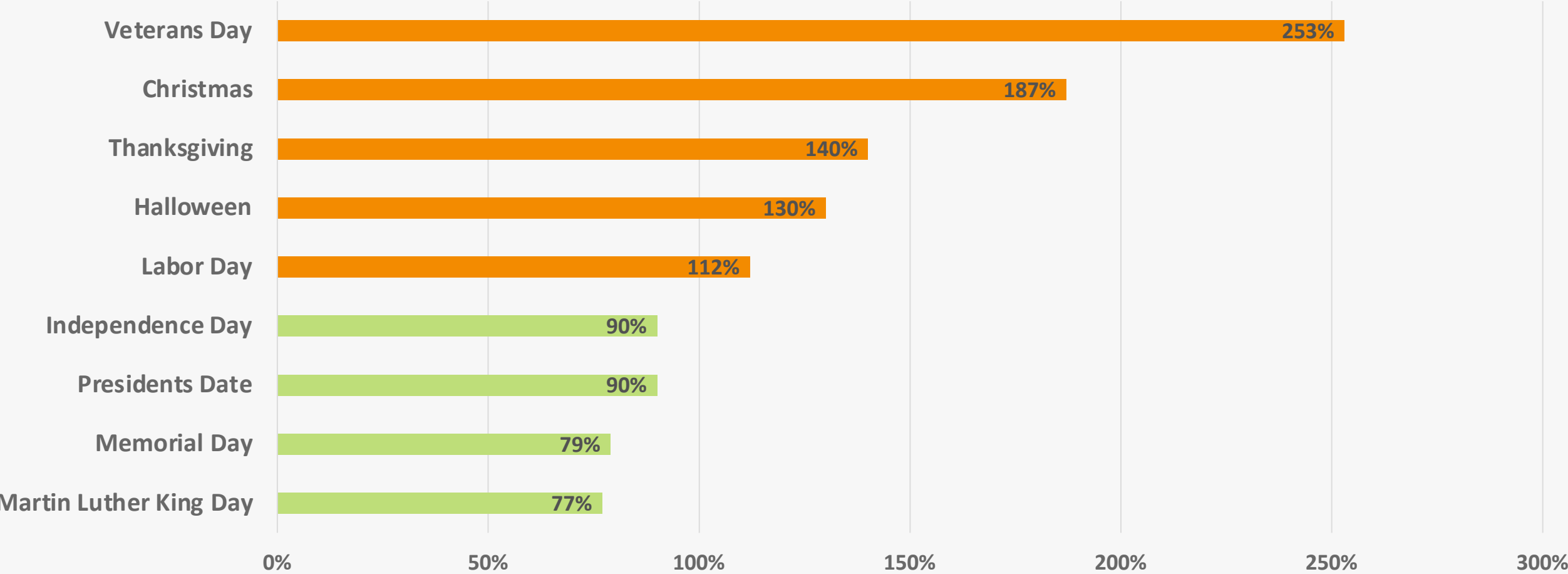
# No Day is Sacred - Ransomware

Day of Week Ransomware Detonation



# No Day is Sacred - Breaches

Holiday Window Percent of Average Daily Breach Event Rate  
2012 - 2021



# Don't Assume that Ransomware Victims Will Suddenly Improve



# Don't Assume that Ransomware Victims Will Suddenly Improve

	Observed Change – 1 Year Later
<b>Software Patching Issues</b> Software vulnerabilities with CVSS-rating of Medium or Higher (7.0-10)	<b>15% Better</b>
<b>Unsafe Network Services</b> Internet-exposed unsafe services such as databases and remote administration	<b>50% Worse</b>
<b>Application Security Issues</b> Missing common security practices in applications that collect sensitive data	<b>50% Worse</b>
<b>Web Encryption Issues</b> Errors in encryption configuration in systems that collect and transmit sensitive data	<b>2% Worse</b>
<b>Email Security Issues</b> Security issues in active email servers and domains that increase susceptibility to phishing and data theft	<b>22% Better</b>





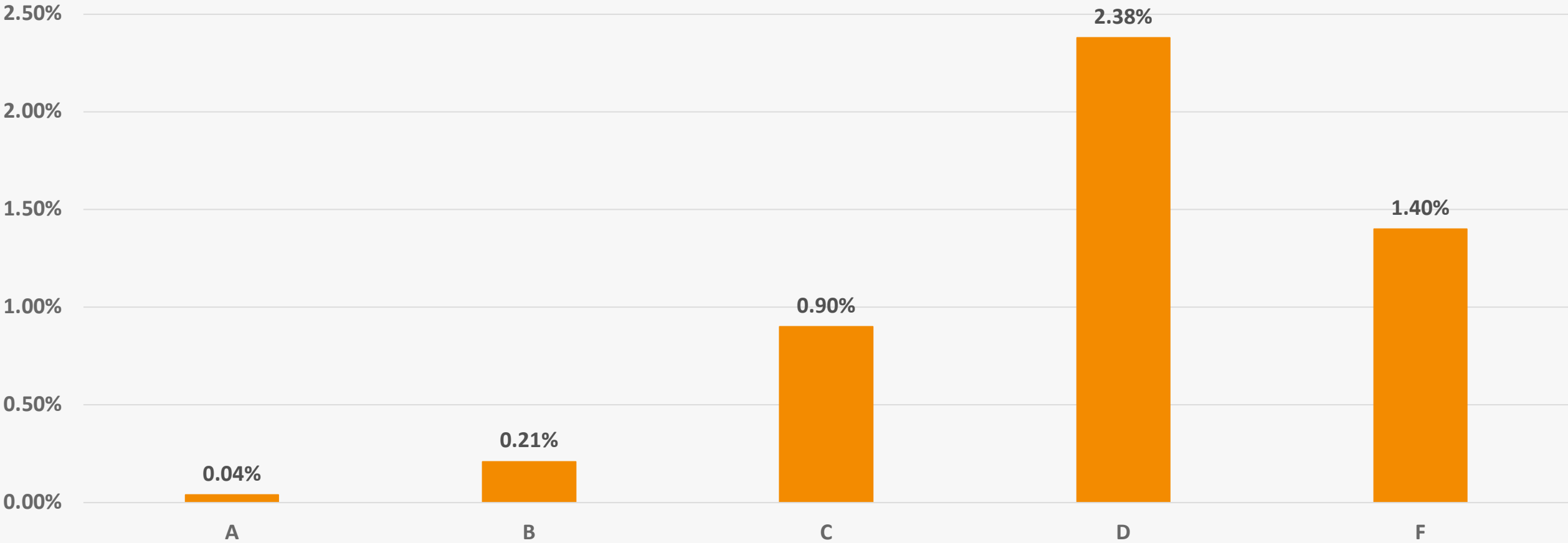
Do One Thing

# Do Business with Companies with Good Cyber Hygiene



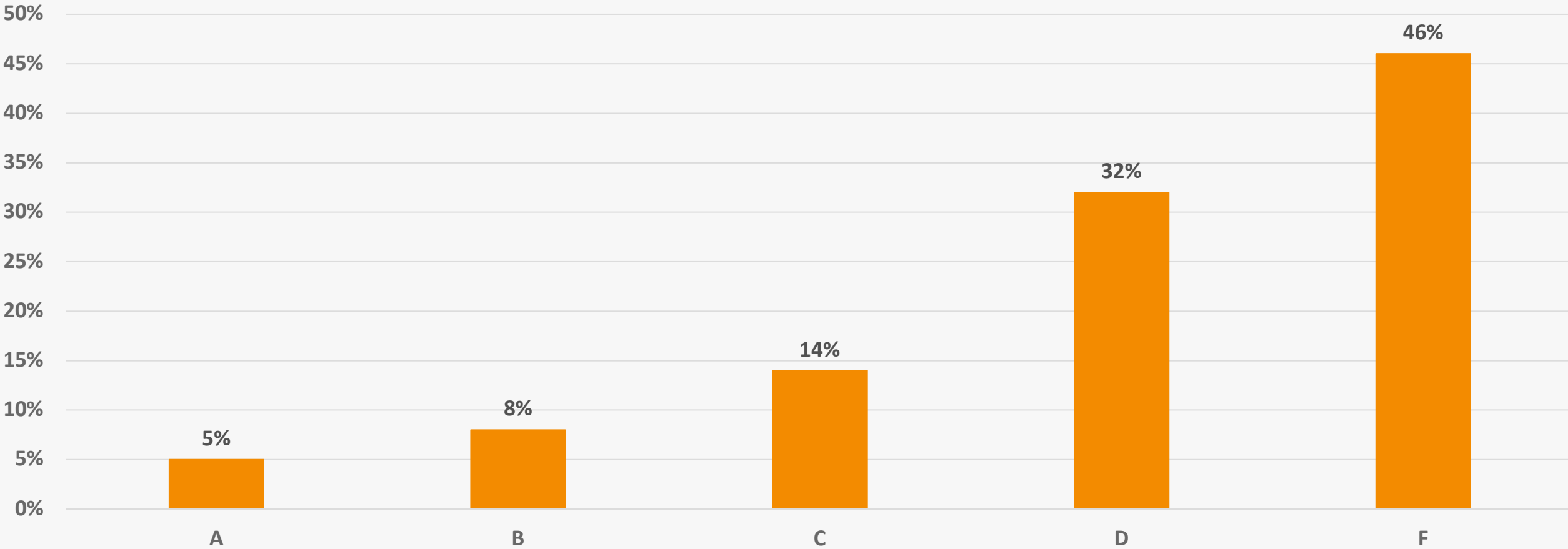
# Do One Thing: Do Business with Companies with Good Cyber Hygiene

Percent of Companies Publicly Reporting Destructive Ransomware Event Since 2016



# Do One Thing: Do Business with Companies with Good Cyber Hygiene

Percent of Companies Publicly Reporting Breach Events Since 2012

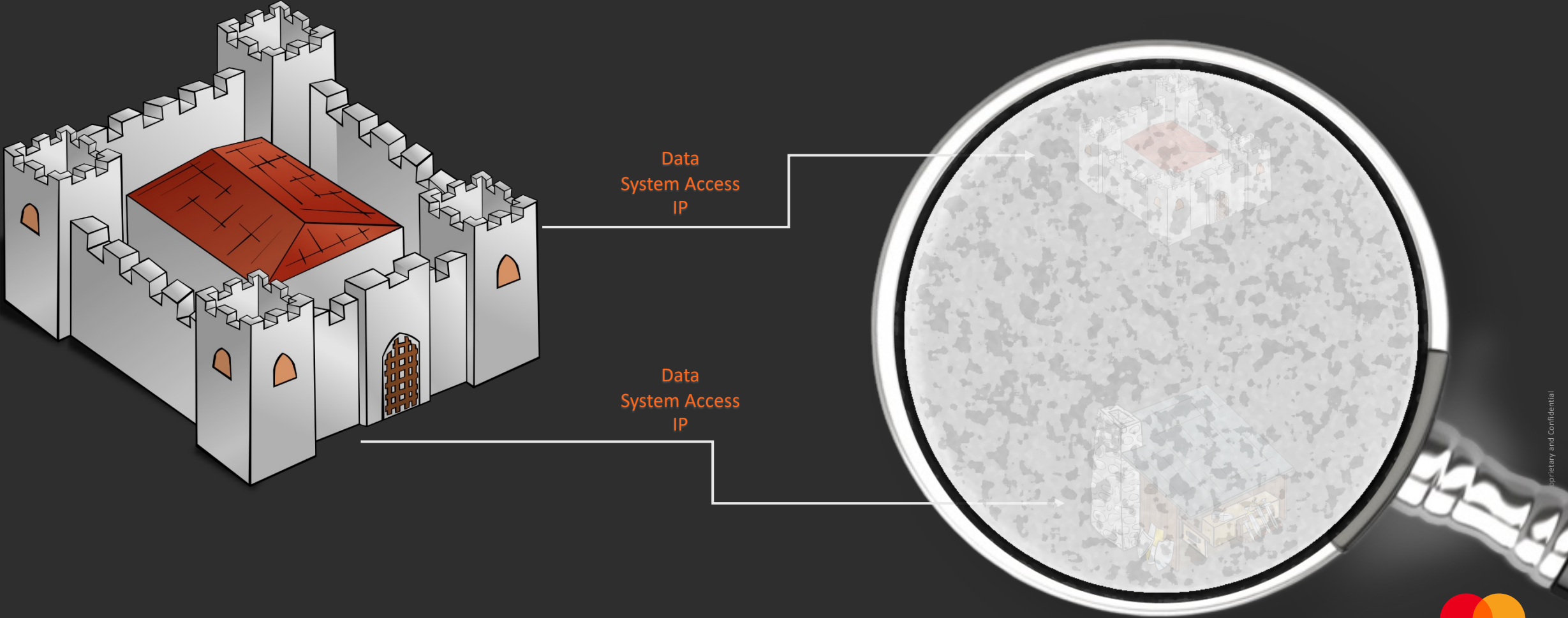




How can we attempt to predict where ransomware or breaches will impact our supply chain?

By gaining situational awareness....

# Why We Do Third-Party Risk Assessments?



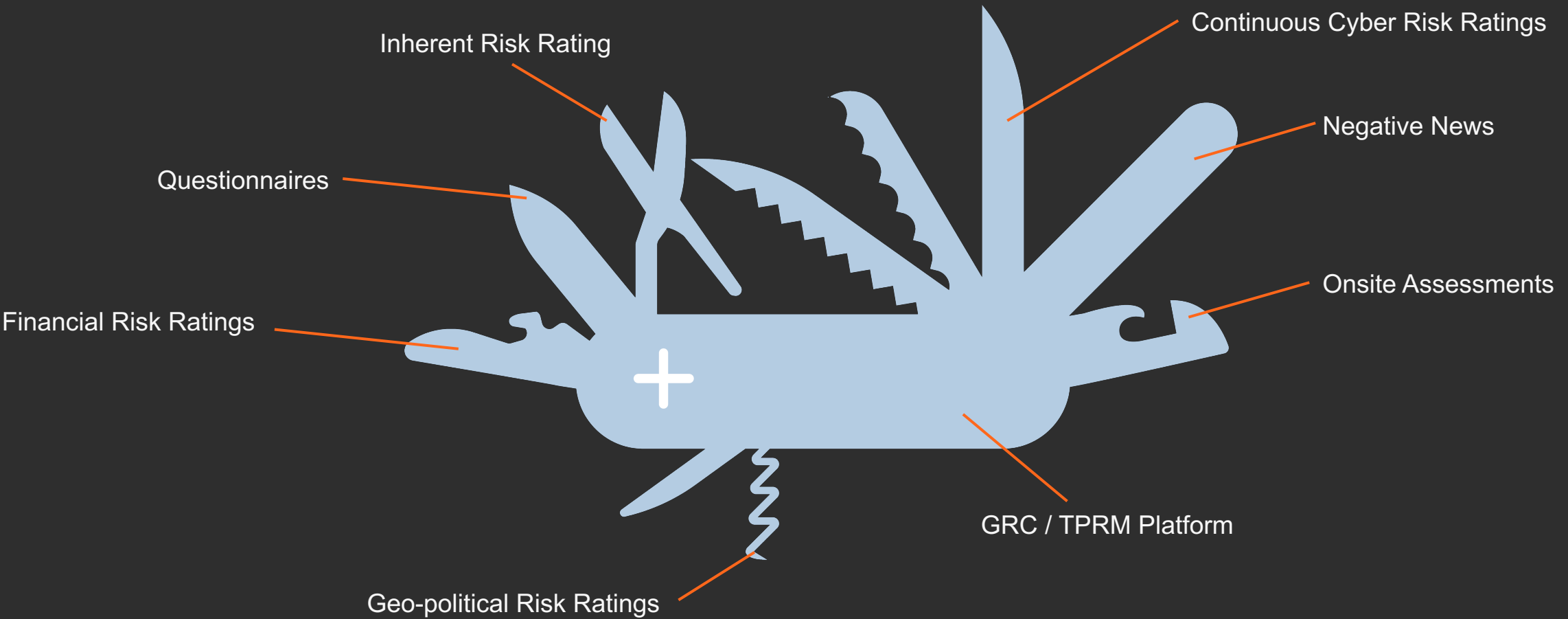
# What Many Third-Party Programs Likely Focus On



# The Flaw In That Thinking

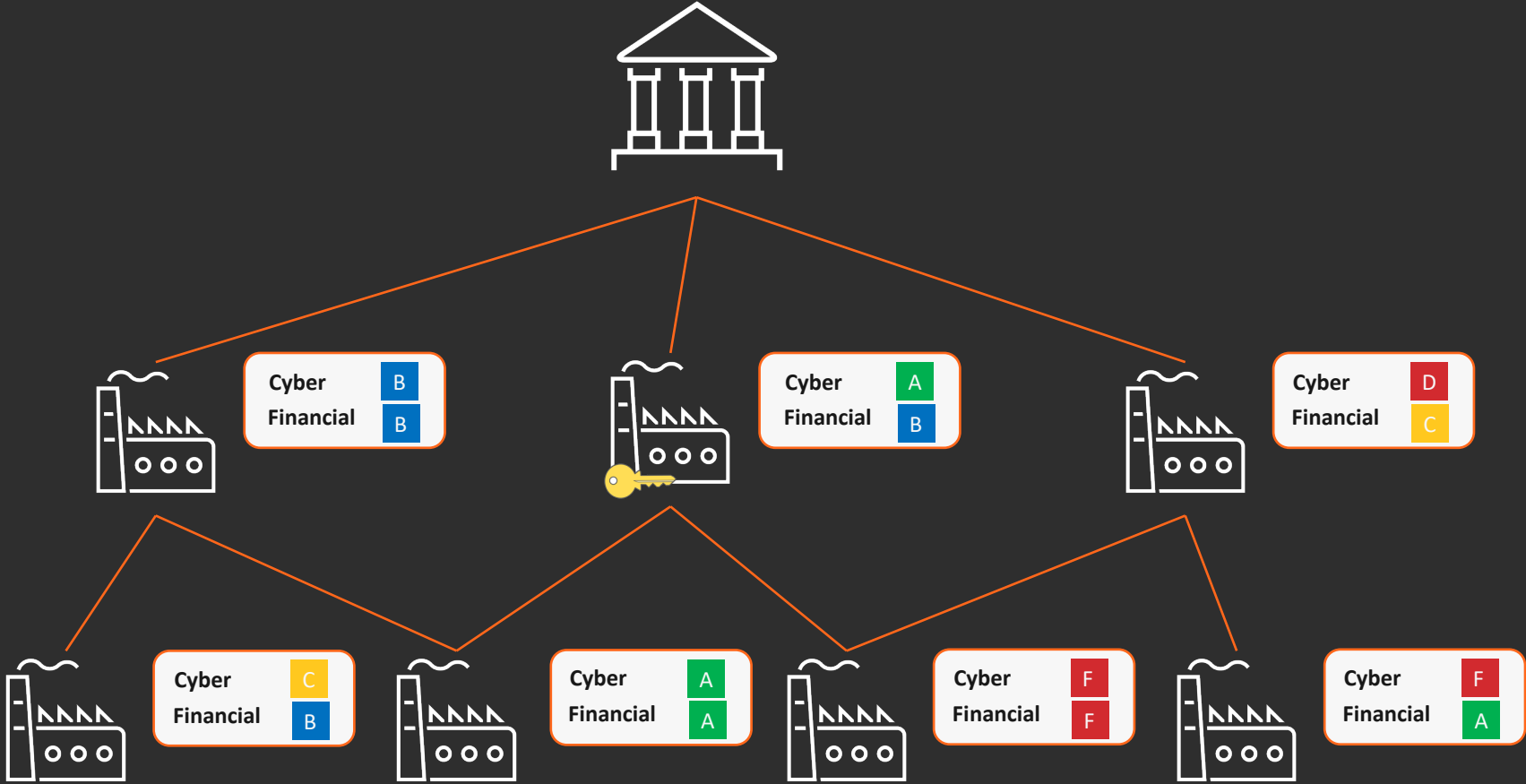


# Designing a TPRM Program for Situational Awareness





# Utilizing Situational Awareness – Who is the Weak Link?



# What the Data Tells Us About Company X

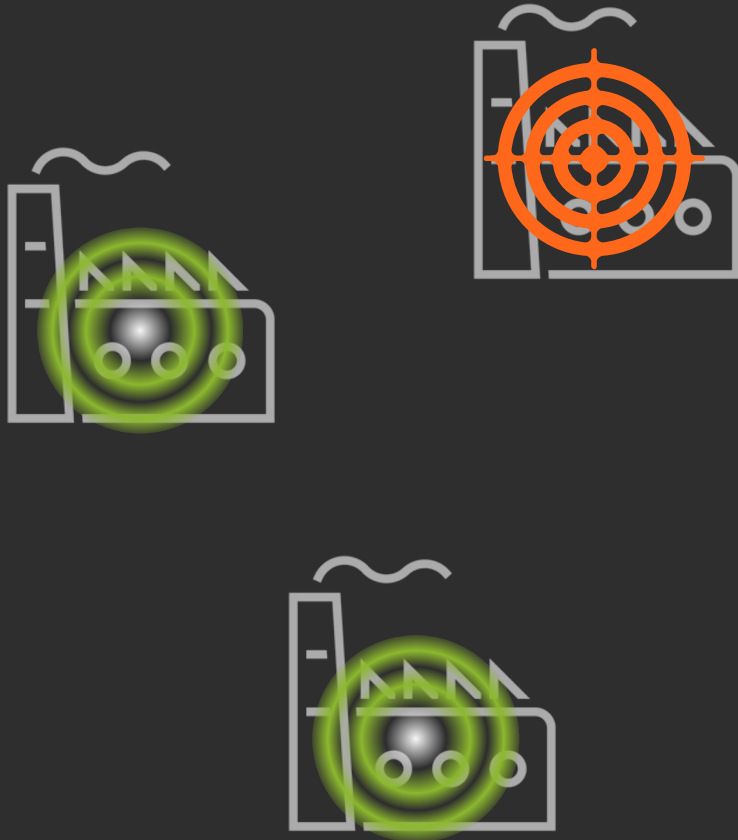


- 40x more likely to experience a Ransomware event<sup>1</sup>
- 4x more likely to experience a breach<sup>2</sup>
- Lower financial health indicates that they may not recover from either event
- Single point of failure for multiple third-party vendors/suppliers
- Relied on by key vendor/supplier – Potential problem area to address ASAP

1- Predicting Ransomware Event Frequency with RiskRecon Cybersecurity Ratings and Insights, <https://www.riskrecon.com/ransomware-event-frequency-report>  
2- Predicting Third-Party Breach Event Frequency with RiskRecon Cybersecurity Ratings, <https://www.riskrecon.com/predicting-breach-frequency>



# How Do We Use This Information?



- TPRM staff resources are not infinite
- Prioritize resources to where real risk resides
- Avoid doing things just because that's how they have always been done
- Bring real results to your TPRM program by working smarter, not always harder



### RiskRecon



- Detailed cyber risk information across various security domains
- Continuous Monitoring for change in risk profile and events
- Actionable risk plans shared with third-party service providers and vendors using the collaboration portal

### Systemic Risk Assessment

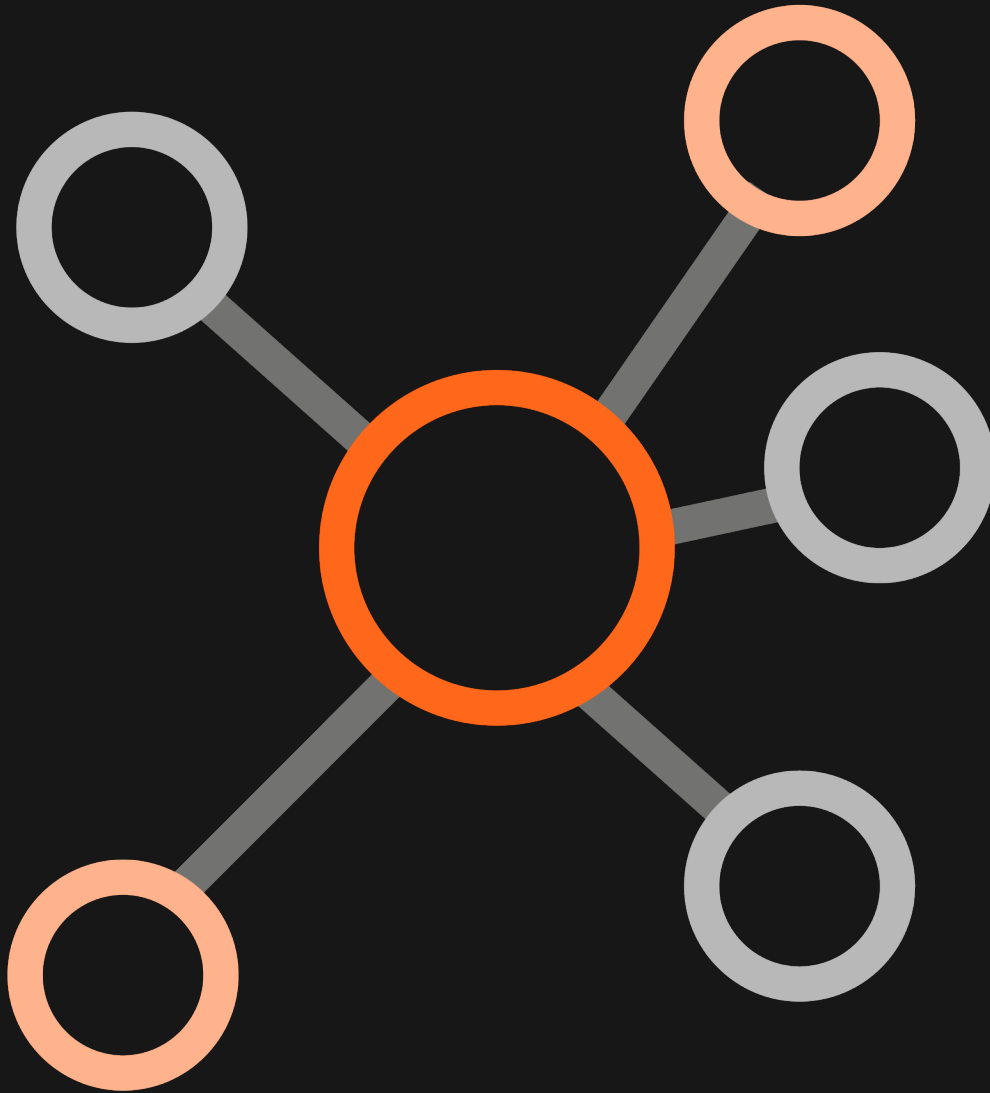


- High level risk score information across various categories – Cyber, Financial, ESG, Geo-political, Restrictions, Operational
- Over 330 million unique entities sourced from public, academic, government and commercial data sets
- Continuous Monitoring for change in risk profile and events



## In summary

- We must build third-party and supply chain risk programs to be situationally aware
- By leveraging external cyber hygiene intelligence, we can make predictions about which vendors are most likely to experience breach or ransomware events
- That information can be combined with what we know about the relationship to determine potential problems
  - What the supplier does for our organization?
  - What is the financial health of the supplier?
  - Are they a key supplier?
- Putting it all together allows us to prioritize finite resources to address potential weaknesses in our supply chain before they interrupt our operations.



# Questions?

[Jonathan.ehret@mastercard.com](mailto:Jonathan.ehret@mastercard.com)

<https://www.linkedin.com/in/ehretjs/>