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

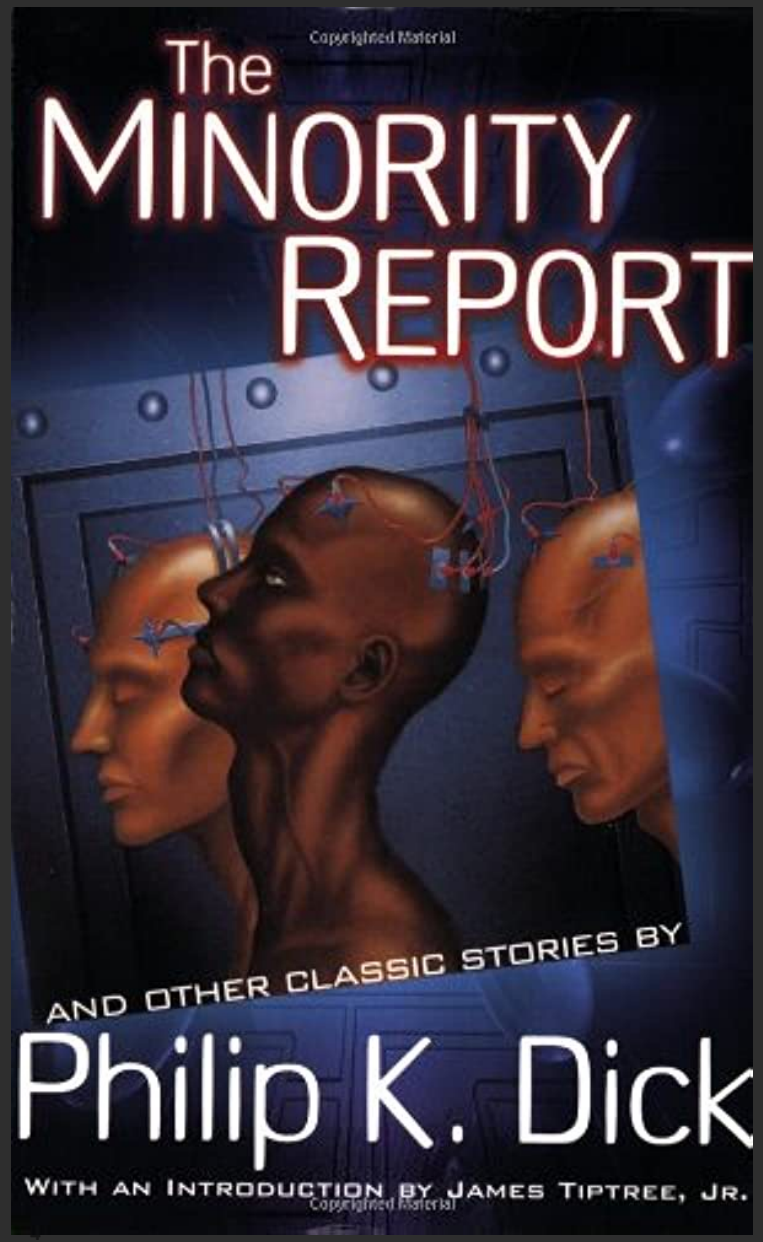
Jon Ehret is Vice President of Customer Enablement for RiskRecon, a Mastercard company. Jon brings 20+ years of experience in technology and risk, including extensive experience building, maturing and running third party risk programs in both the finance and healthcare industries.

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?

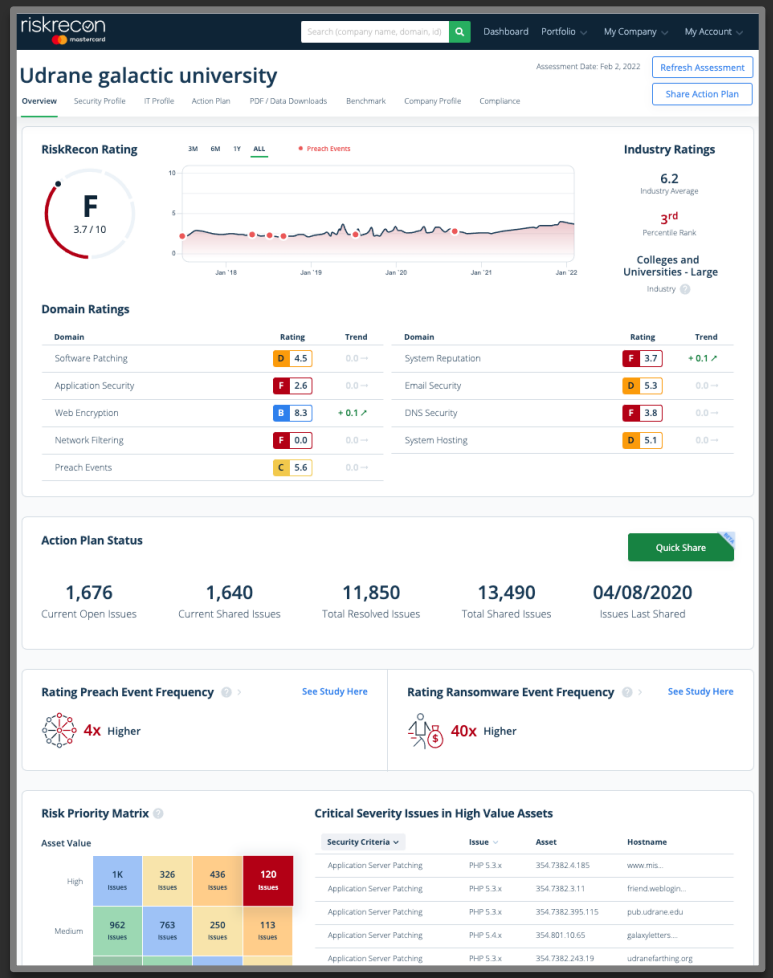


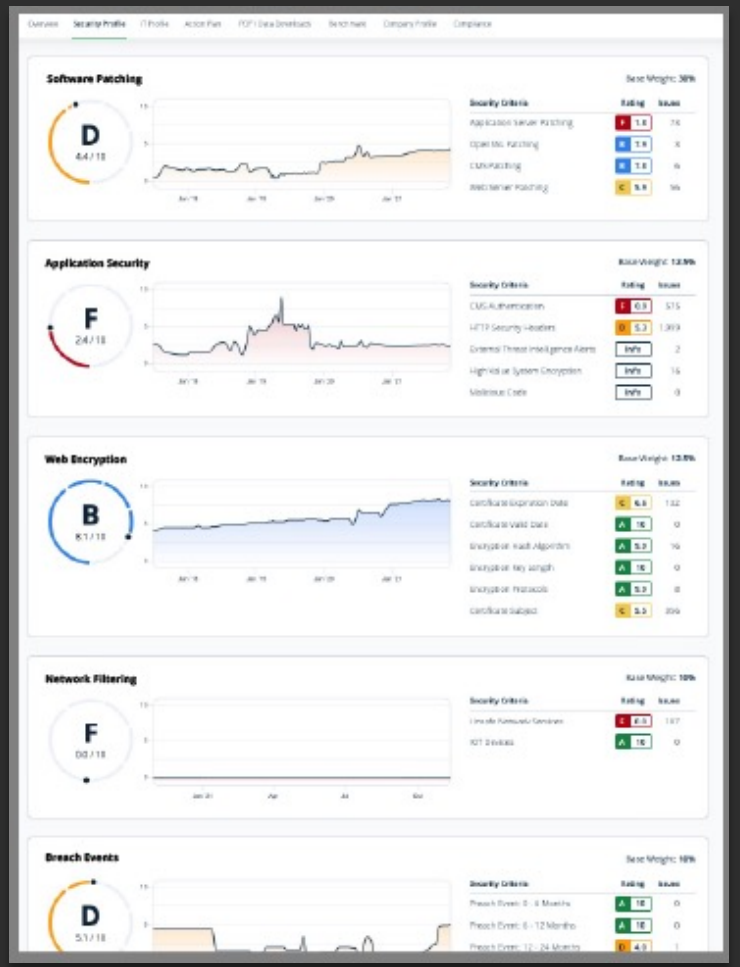
- Classic Science Fiction novel written by Philip K. Dick
  - Made into a Hollywood movie starring Tom Cruise
- Premise:
  - Crime in the future is fought before it happens. ”Precogs”, mutants with the ability to see the future, are utilized by the PreCrime division to identify people who will commit 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…..

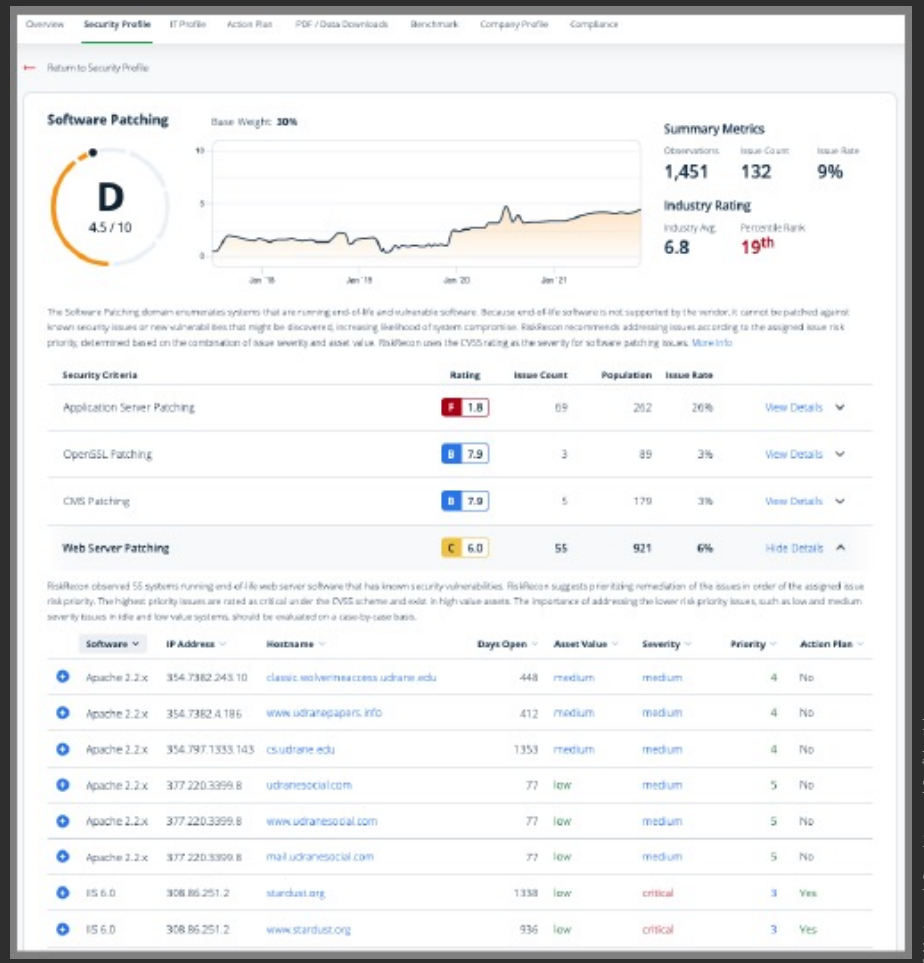
What Data Did We Look At?

- 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





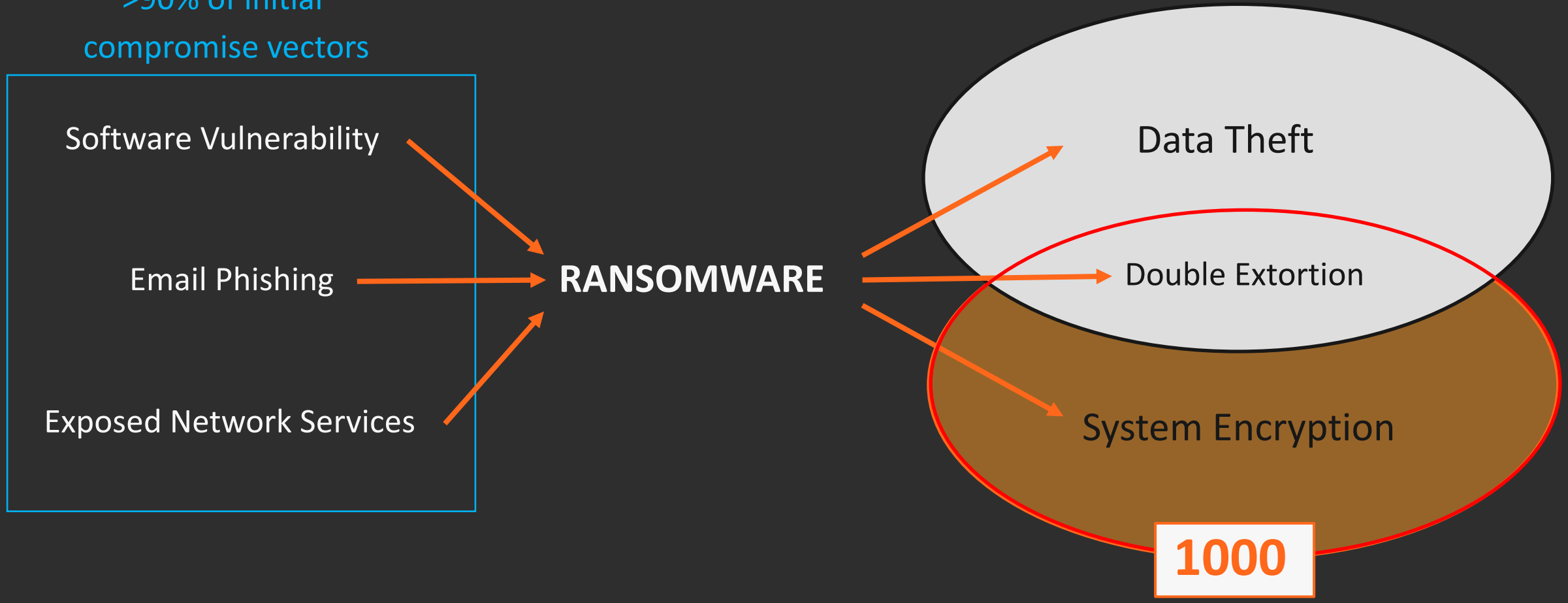


Assessing and Rating ~15M Entities Worldwide

RiskRecon Ransomware Study

Publicly-Disclosed Events
January 2016 – March 2022

>90% of initial compromise vectors

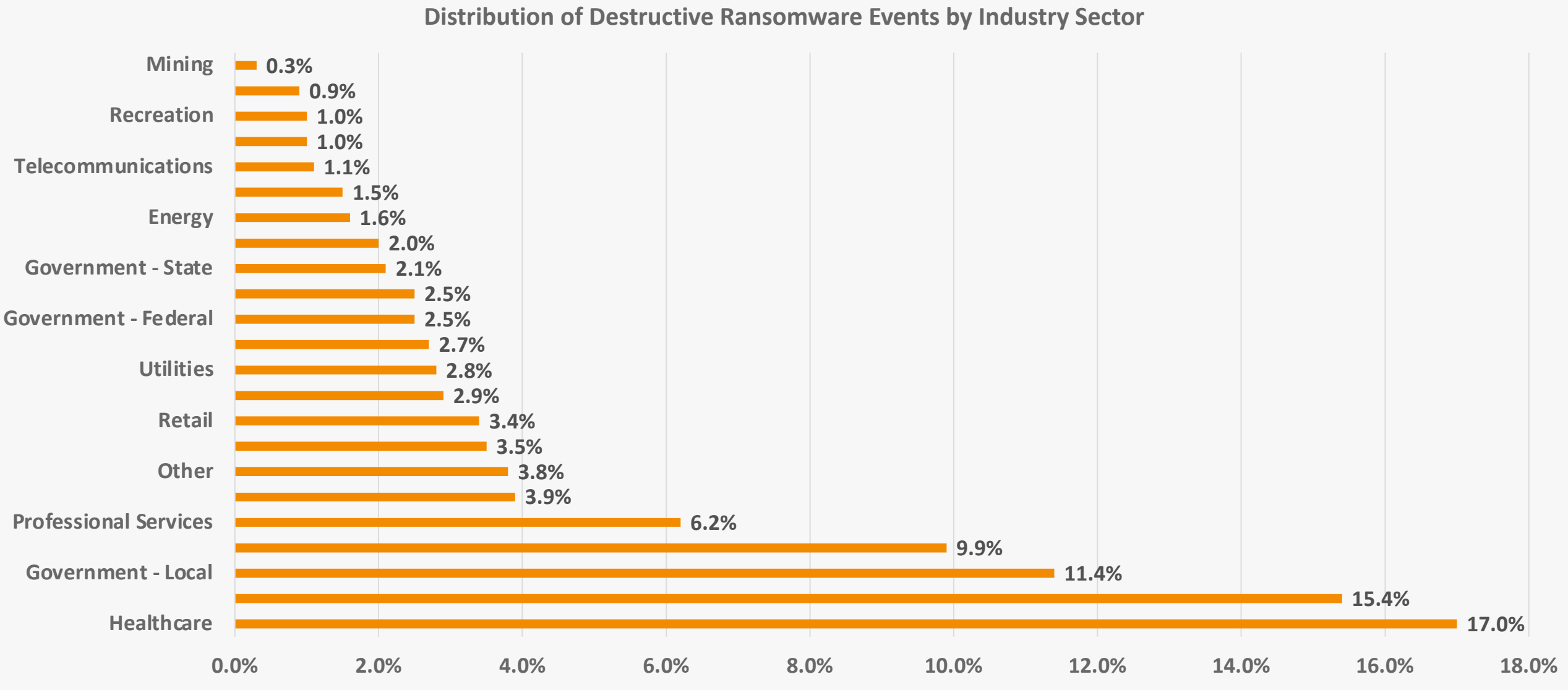


RiskRecon Breach Study

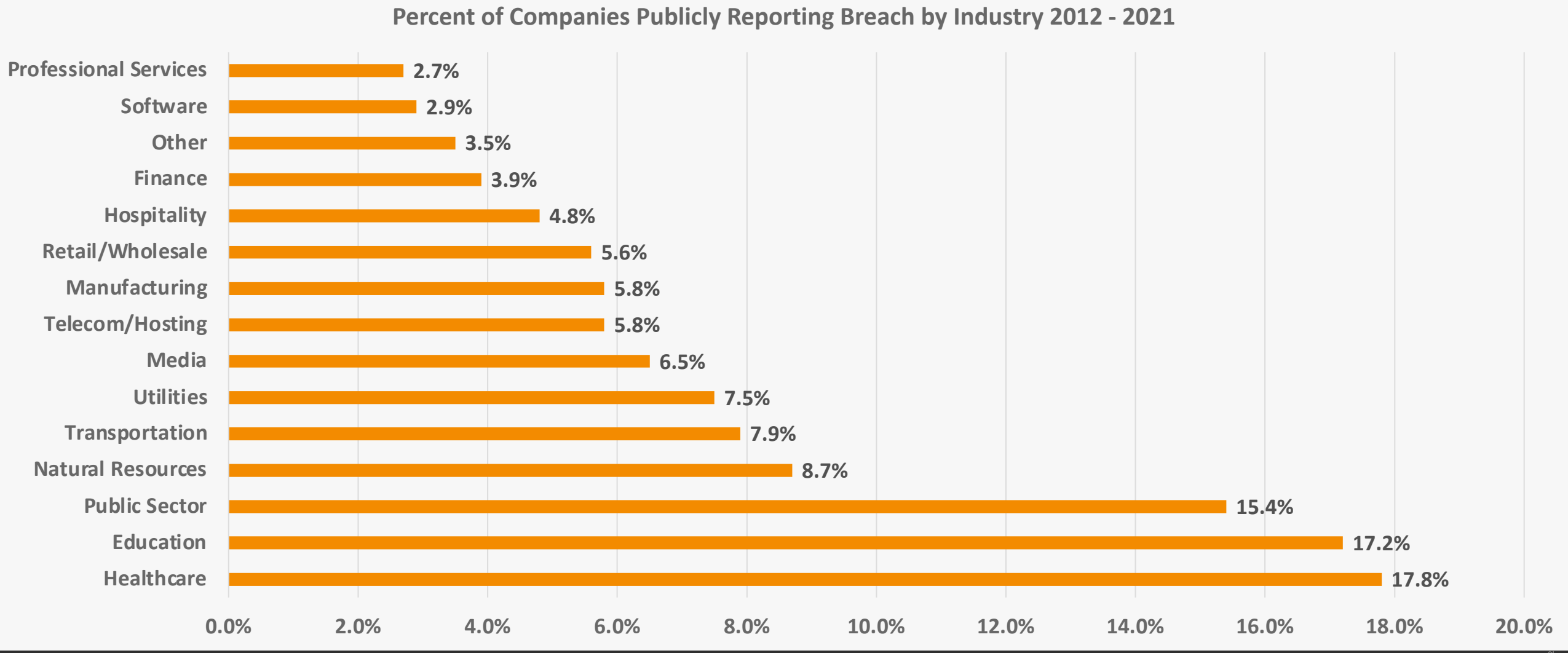
- Sample Size: 109,000 companies
- Breaches Reviewed: 8,892
- Range: Jan 2012 – Dec 2021
- Publicly Disclosed Events Only

Lesson

Everyone is a Target

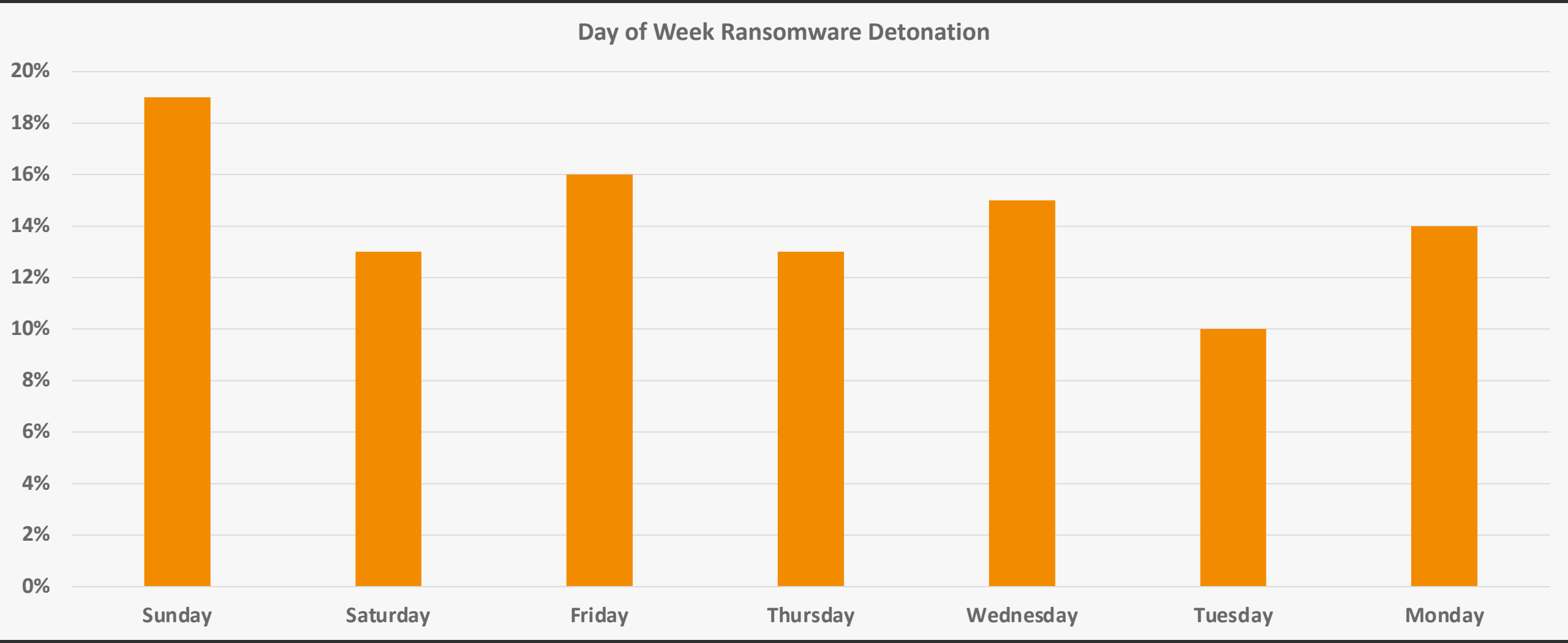


Everyone is a Target

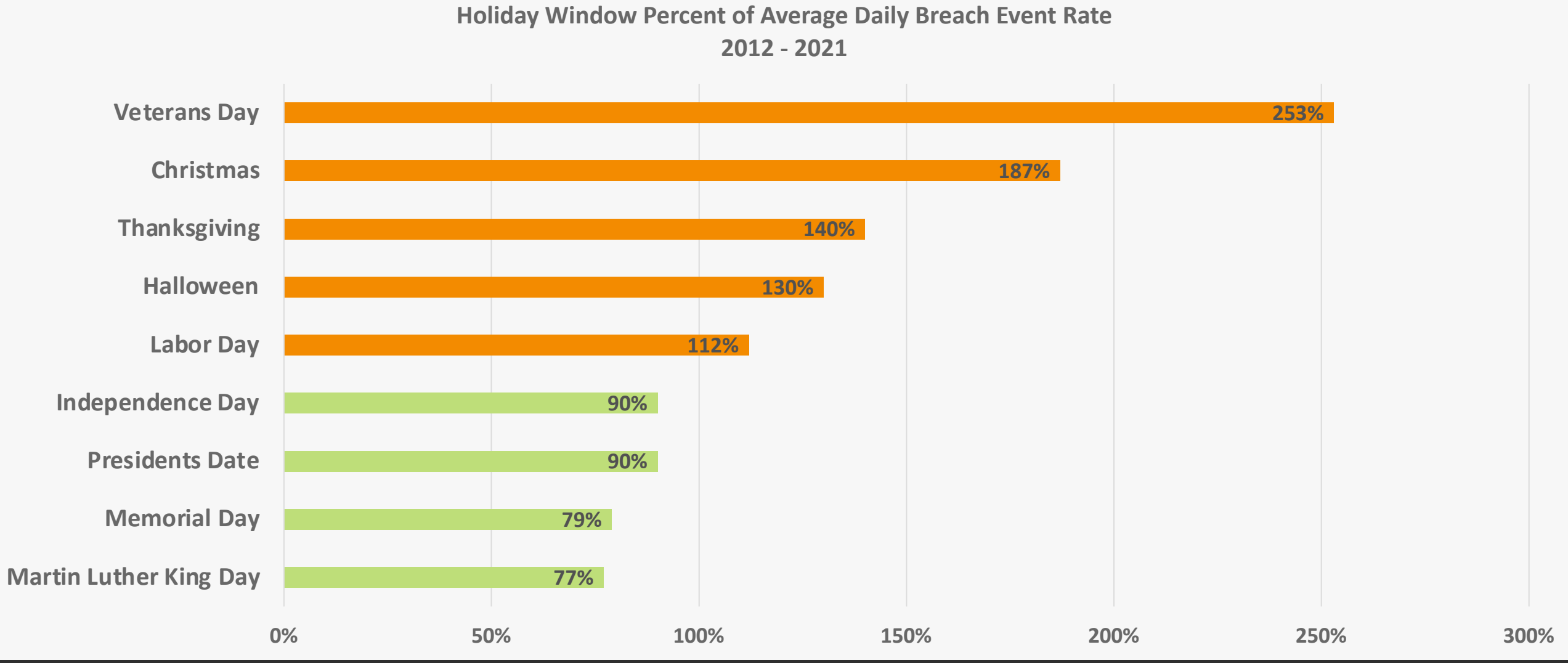


Lesson

No Day is Sacred - Ransomware



No Day is Sacred - Breaches

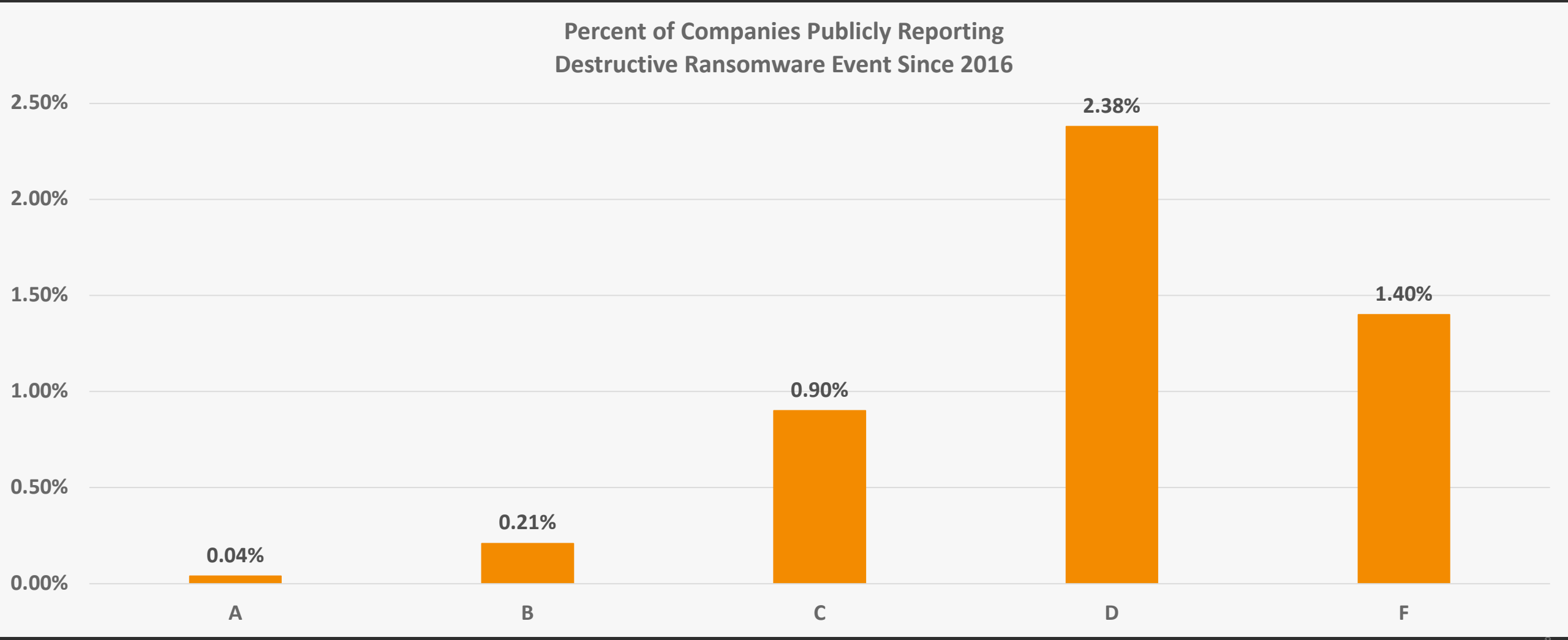


Don’t Assume that Ransomware Victims Will Suddenly Improve

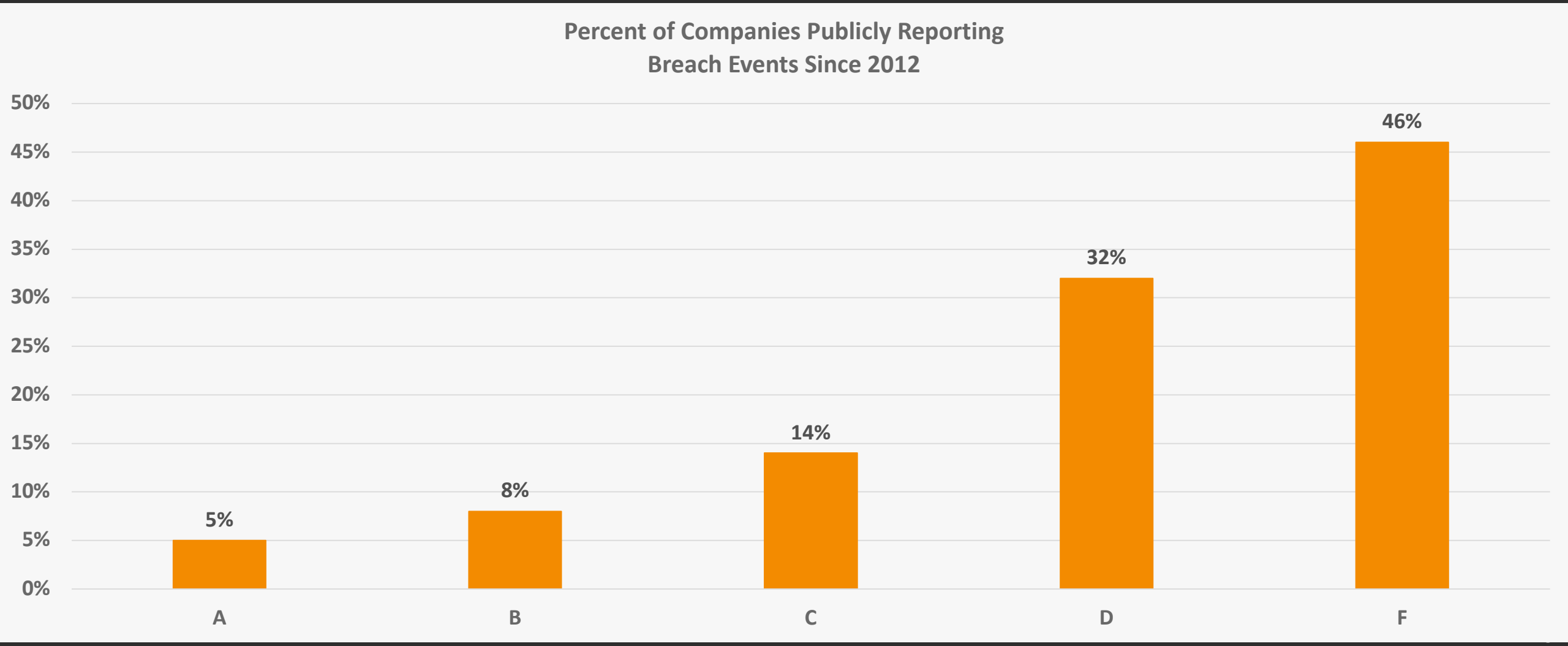
Don’t Assume that Ransomware Victims Will Suddenly Improve

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

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



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

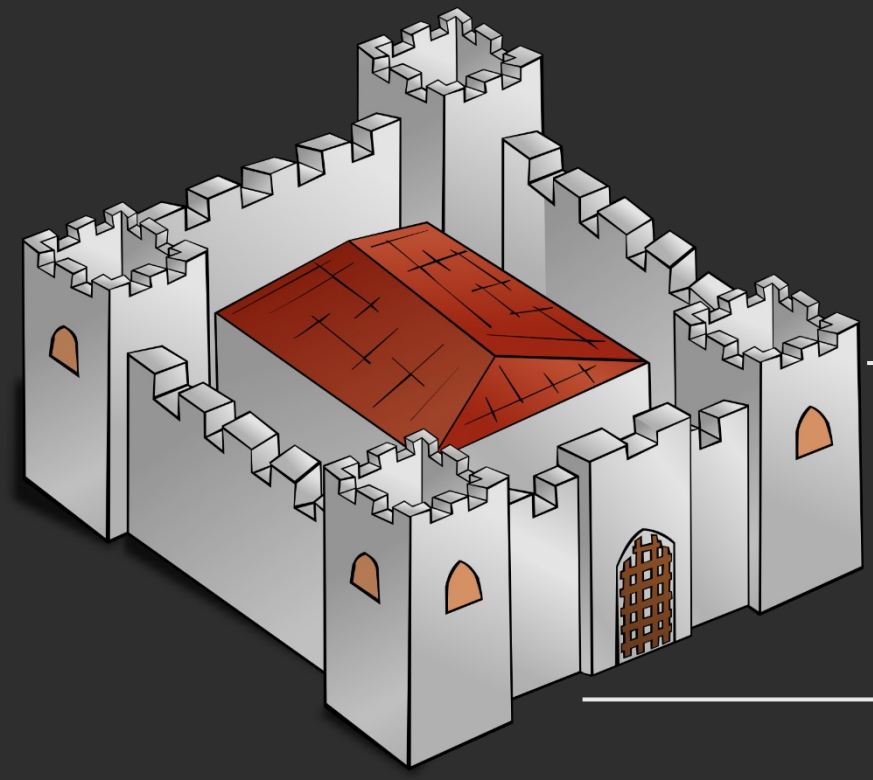


Question

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

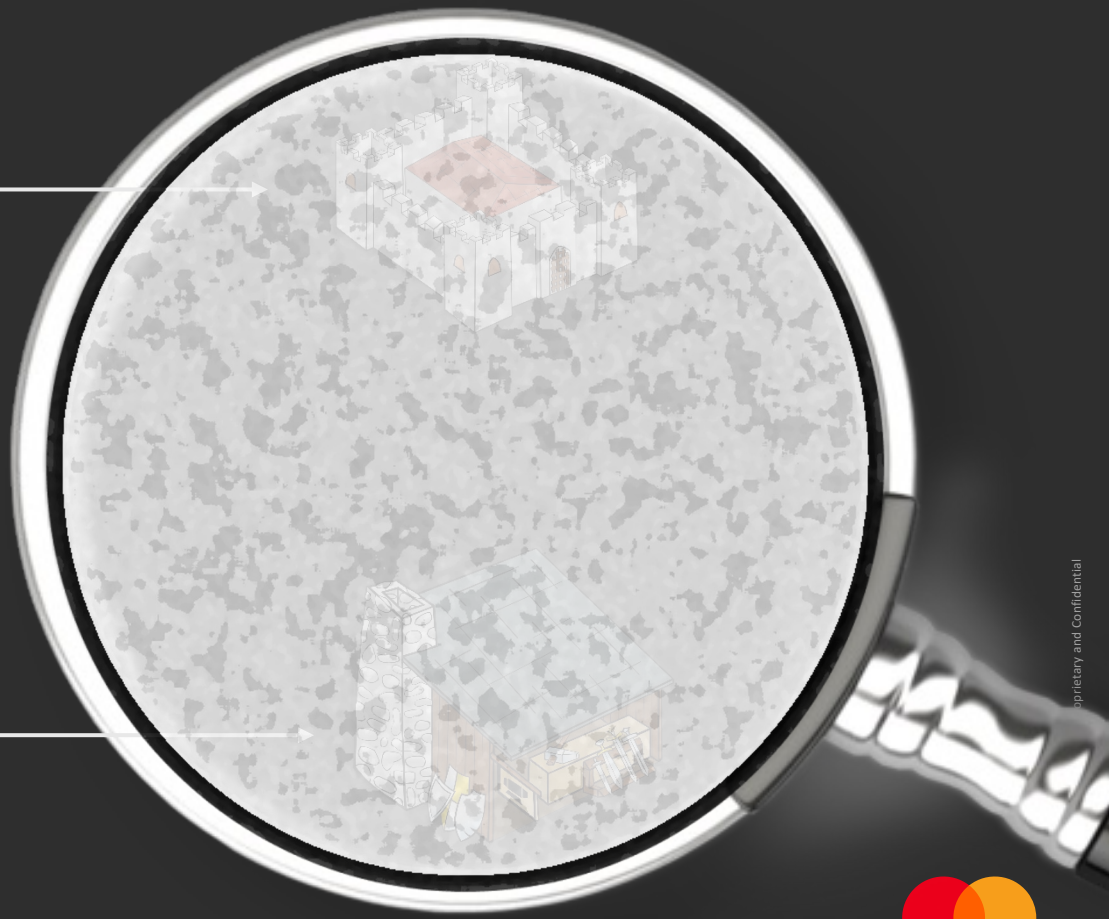
By gaining situational awareness….

Why We Do Third-Party Risk Assessments?



Data
System Access
IP

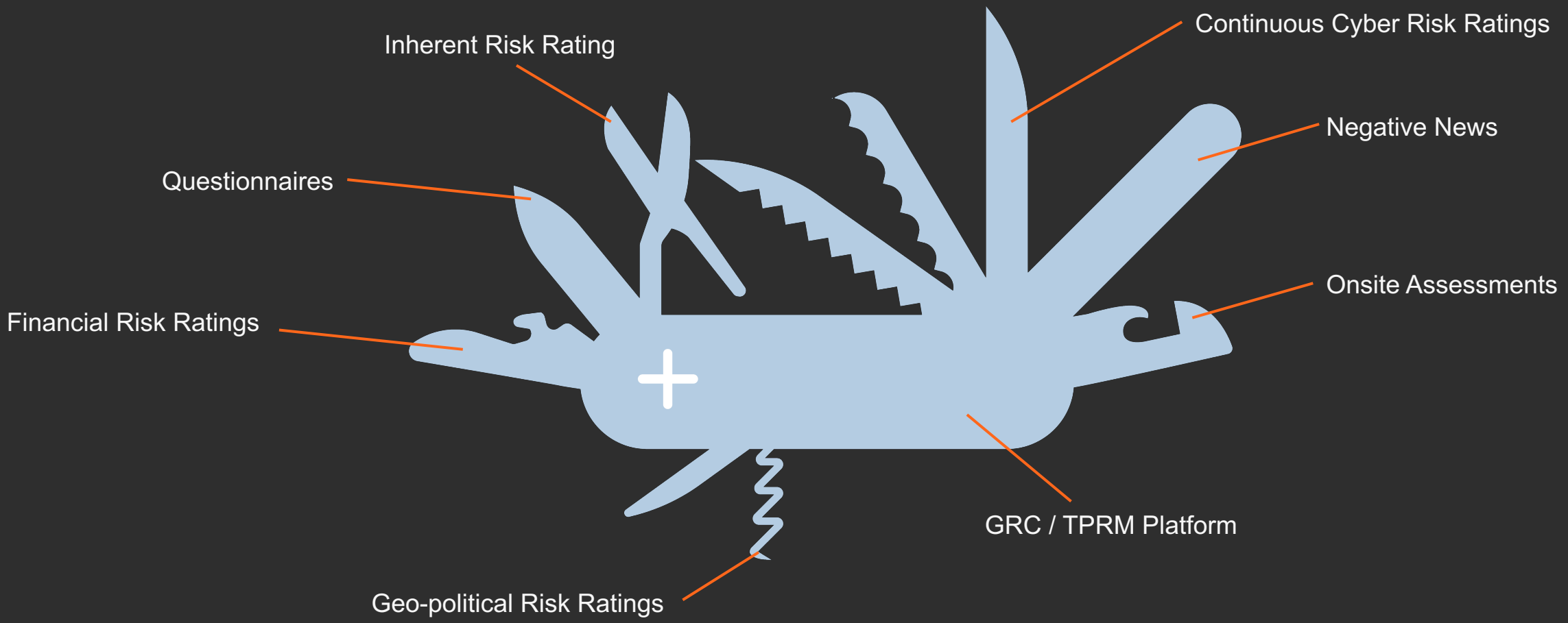
Data
System Access
IP



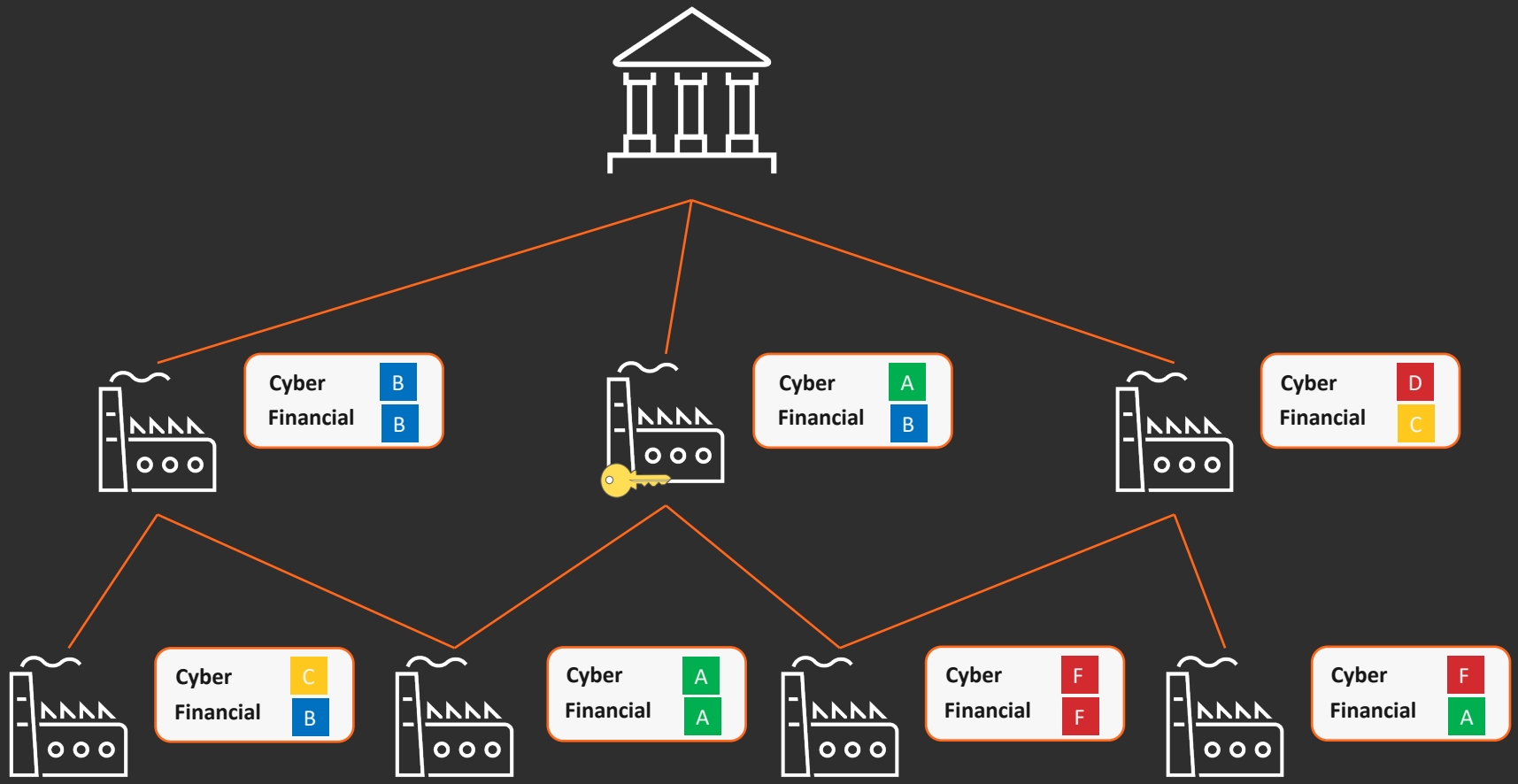
What Many Third-Party Programs Likely Focus On

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

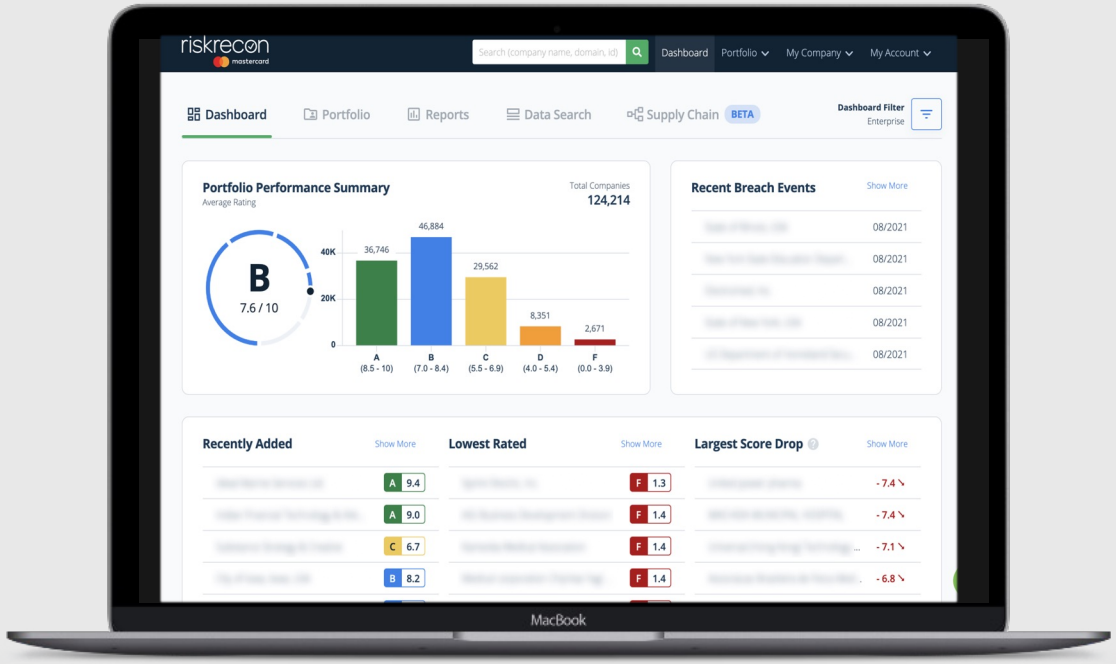
- 40x more likely to experience a Ransomware event[1]
- 4x more likely to experience a breach[2]
- Lower financial health indicates that they may not recover from either event
- Single point of failure for multiple third-party vendors/suppliers
- Relied on by key vendor/supplier – Potential problem area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

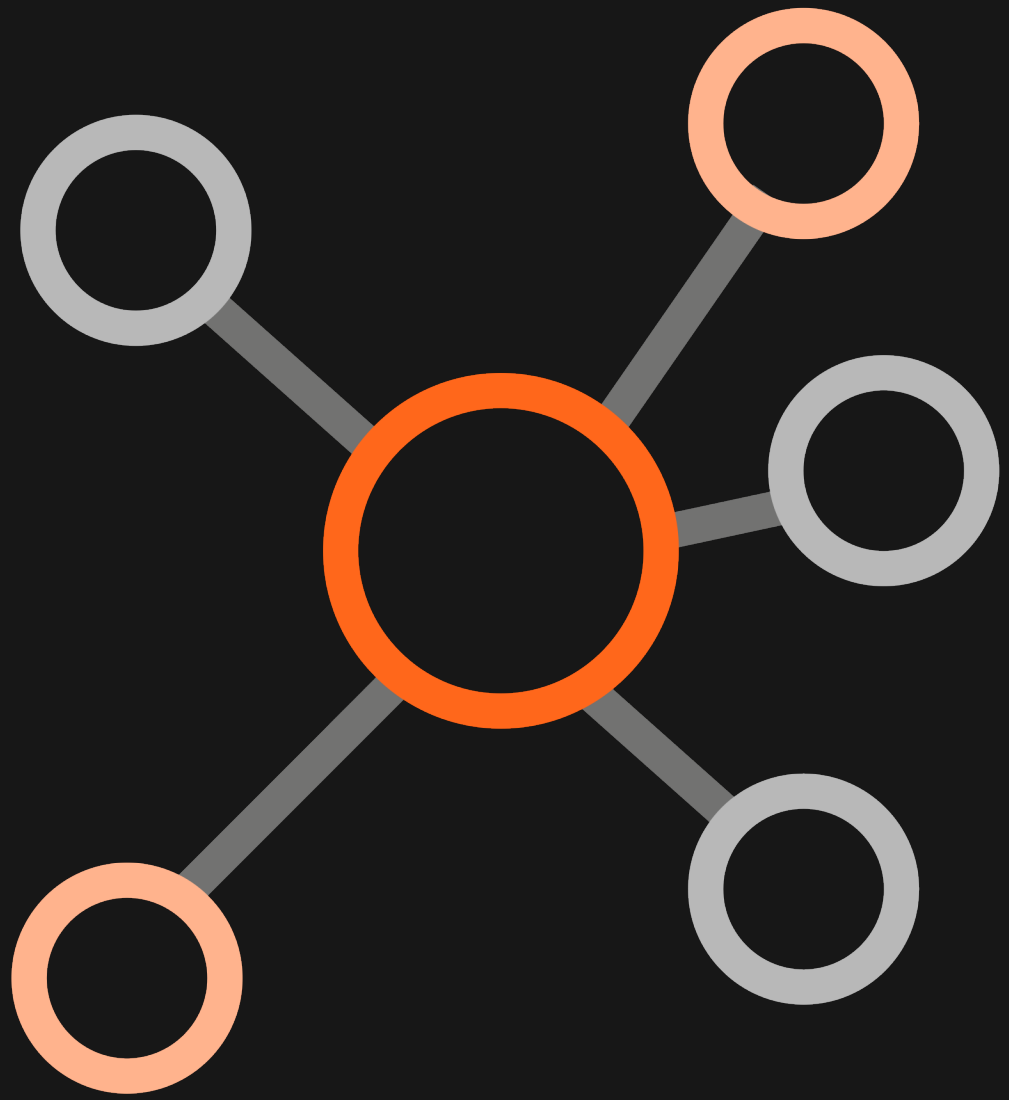
RiskRecon



- → 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

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