Threat Forecasting

Using Open Source Data to Foresee Your Next Breach

Today’s Topics

THREAT FORECASTING IS POSSIBLE

THE WORLD SHALL BECOME KNOWN TO YOU

HOW TO FORECAST IN RISK ASSESSMENTS

Duty of Care Risk Analysis

Impact *(Others)* **x Likelihood**

Impact *(You)* **x Likelihood**

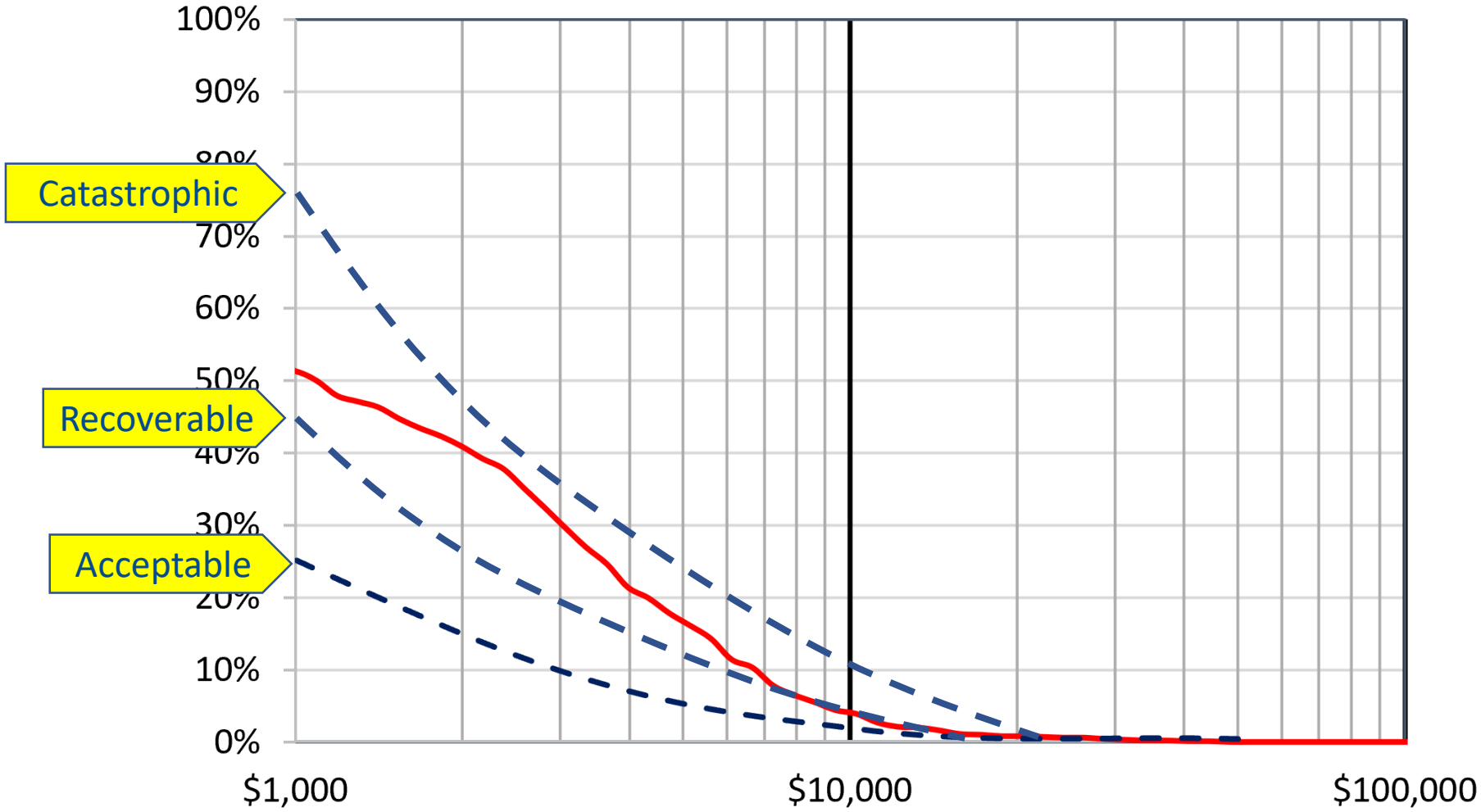
DoCRA

"Risk only to me? What about balance?"

Risk	=	Objectives Impact	Mission Impact	Obligations Impact	x	Likelihood
		"Profit"	*"User health"*	*"Others"*		
12	=	*3*	*2*	***4***	*x*	***3***
		1. On plan	*1. Significant results*	*1. No harm*		*1. Not possible*
		2. Within variance	*2. Few flat results*	*2. Concern*		*2. Rare, if at all*
		3. Out of variance	*3. Significant misses*	*3. Few embarrassed*		*3. Occasional*
		4. < 3 yrs profit loss	*4. Majority misses*	*4. Many exploited*		*4. Common*
		5. Out of business	*5. Cannot help users*	*5. Millions exploited*		*5. Frequent*

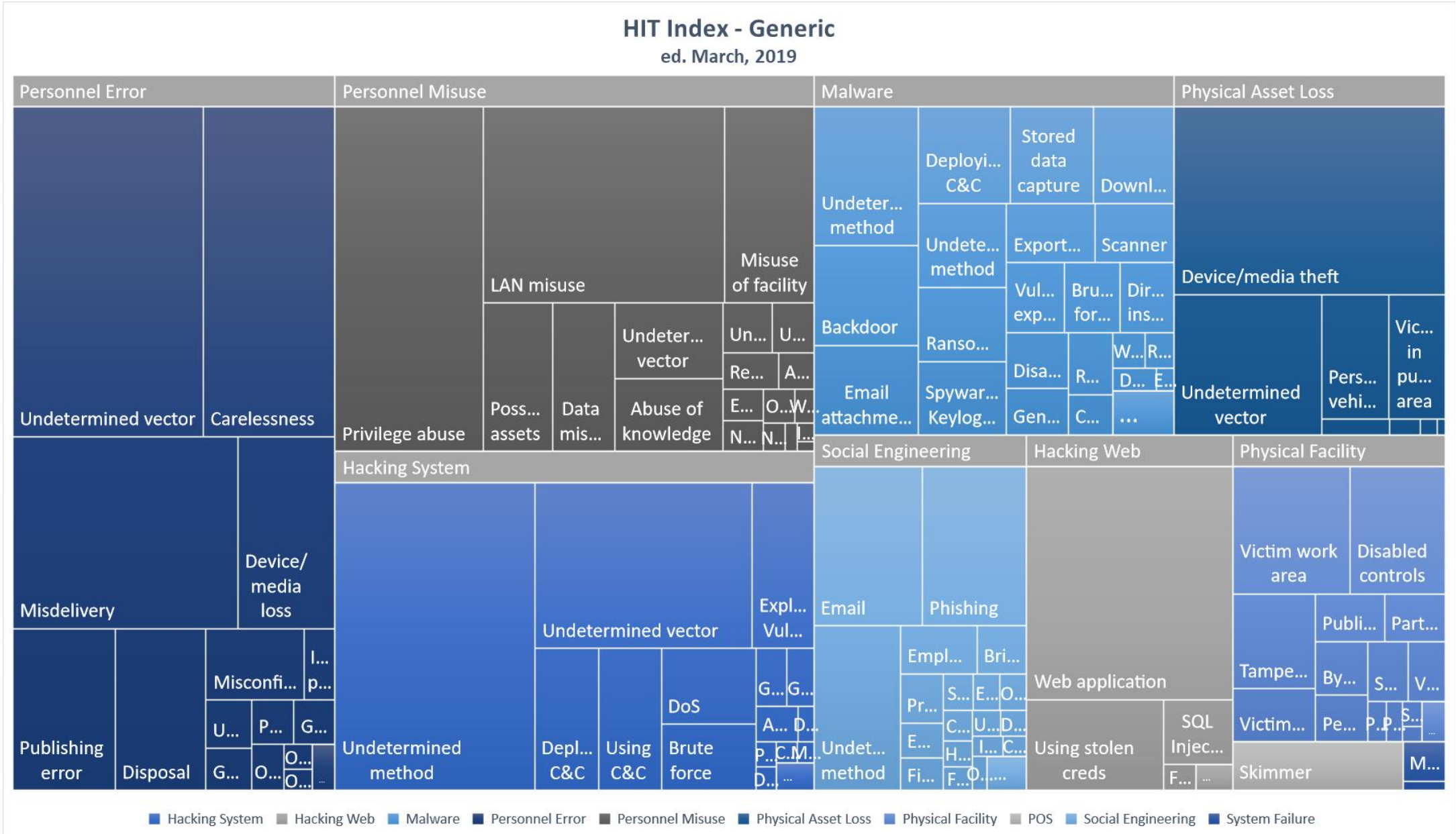
* Risk criteria for a Social Health App

(*for quants, indicate limits along your curve*)



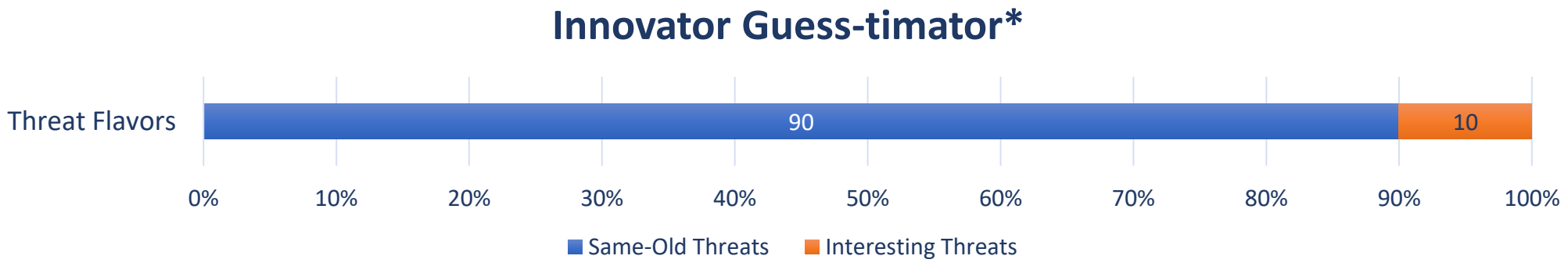
* Courtesy Hubbard Decision Research

What about likelihood?


HIT Index - Generic
ed. March, 2019
Personnel Error
Undetermined vector
Carelessness
Misdelivery
Device/ media loss
Misconfi...
Publishing error
Disposal
Personnel Misuse
Privilege abuse
LAN misuse
Misuse of facility
Poss... assets
Data mis...
Undeter... vector
Abuse of knowledge
Malware
Undeter... method
Deployi... C&C
Stored data capture
Downl...
Backdoor
Undete... method
Export...
Scanner
Ranso...
Vul... exp...
Bru... for...
Dir... ins...
Email attachme...
Spywar... Keylog...
Disa...
Gen...
Physical Asset Loss
Device/media theft
Undetermined vector
Pers... vehi...
Vic... in pu... area
Hacking System
Undetermined method
Undetermined vector
Depl... C&C
Using C&C
DoS
Brute force
Expl... Vul...
Social Engineering
Email
Phishing
Undet... method
Empl...
Bri...
Hacking Web
Web application
Using stolen creds
SQL Injec...
Physical Facility
Victim work area
Disabled controls
Tampe...
Publi...
Part...
By...
Victim...
Pe...
Skimmer
Hacking System
Hacking Web
Malware
Personnel Error
Personnel Misuse
Physical Asset Loss
Physical Facility
POS
Social Engineering
System Failure

"You Can't Predict Cybersecurity Threats!"

- We don't want to *predict*
  - Not going for accuracy
- We want to *forecast*
  - Estimating so we can prepare
- And besides … cybersecurity innovates, but not by much YoY …



* Not a real analysis

Outcomes of Accurate Predictions vs Forecasts

- Results of accurate prediction
  - *“We were breached this year and lost a million records! Just as we predicted!”*

- Results from forecasts
  - *“We saw that Team X was prone to errors, so we removed their access to the crown jewels. Their eventual error released much less data than we originally estimated.”*

Risk is About Likelihood and Impact

Forecasts allow us to either reduce likelihood of effective threats …

… or take systems, data, and people out of harm's way for when the threat happens.

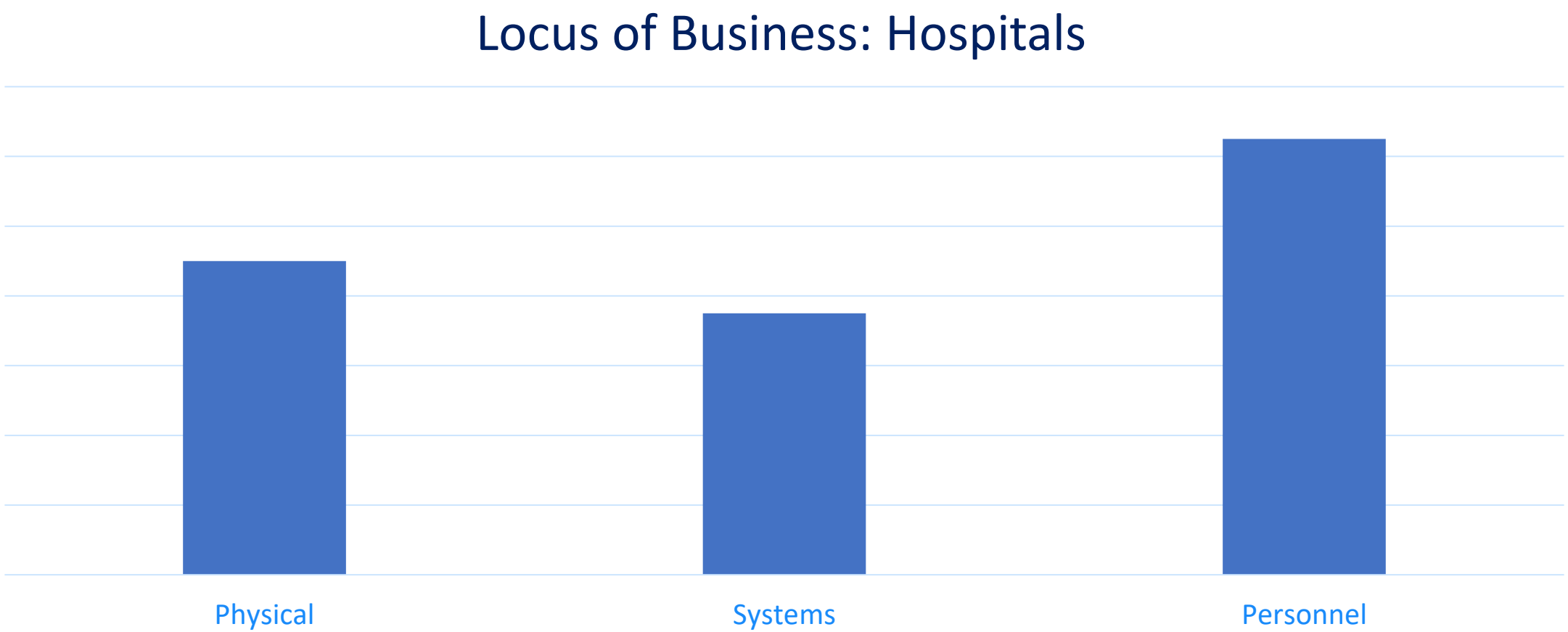
So how do we forecast?

1. Know how your business operates
2. Know your threat landscape
3. Get threat data
4. Align threat data to your threat landscape
5. Organize data to see where threats *have been**

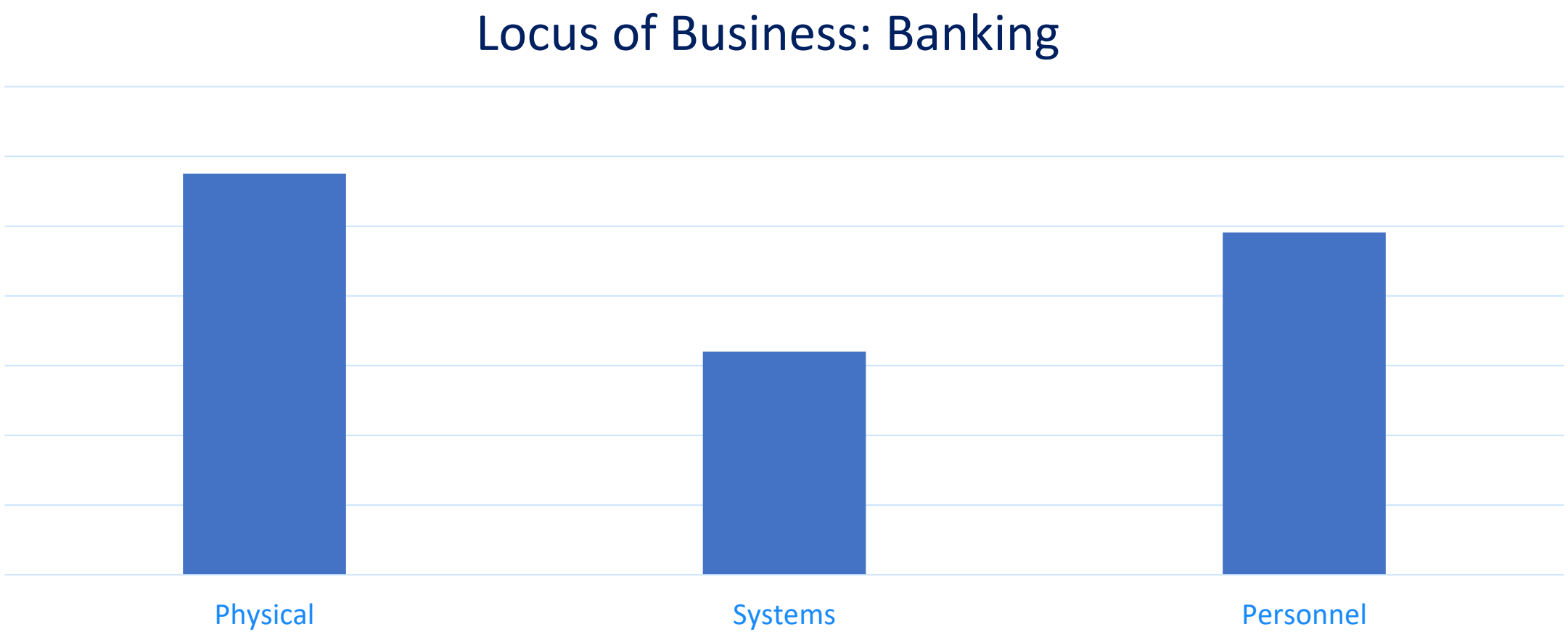
So how do we forecast?

1. Know how your business operates
2. Know your threat landscape
3. Get threat data
4. Align threat data to your threat landscape
5. Organize data to see where threats *have been**

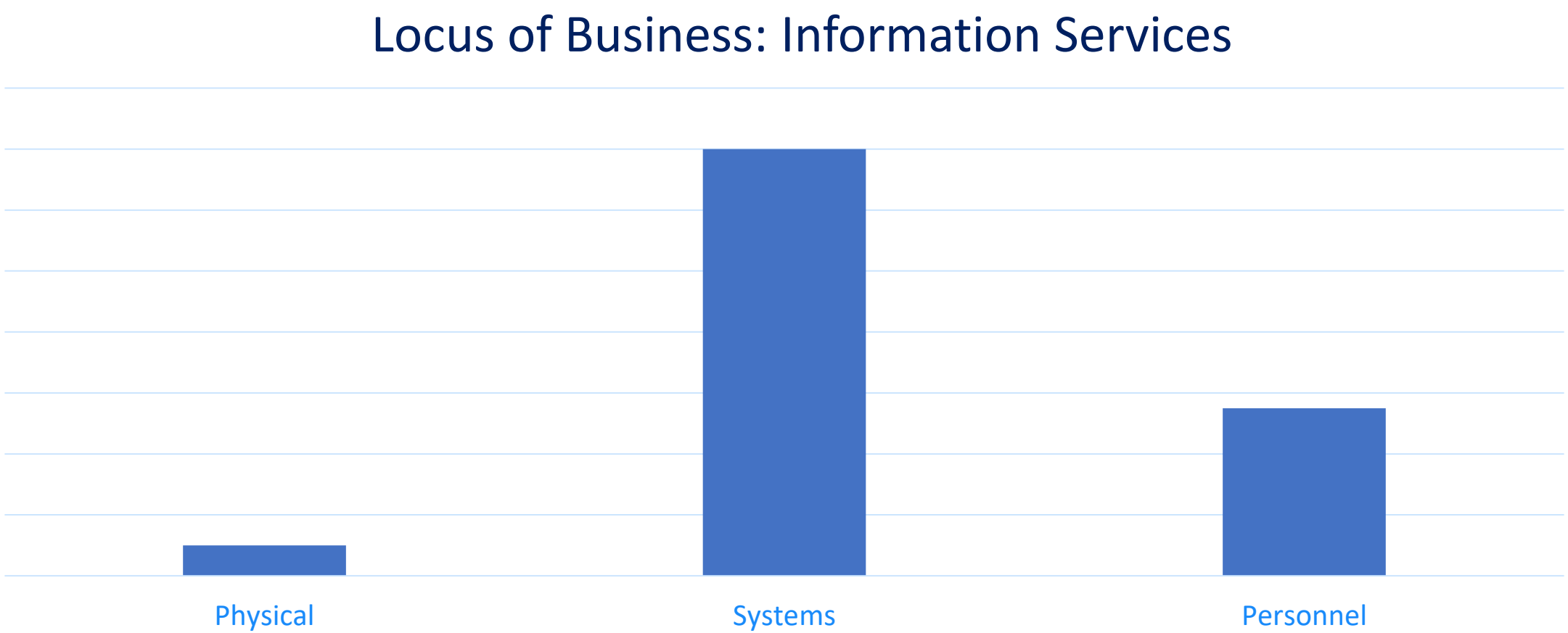
Know Your Business:
Where is Business Conducted/Business Assets?



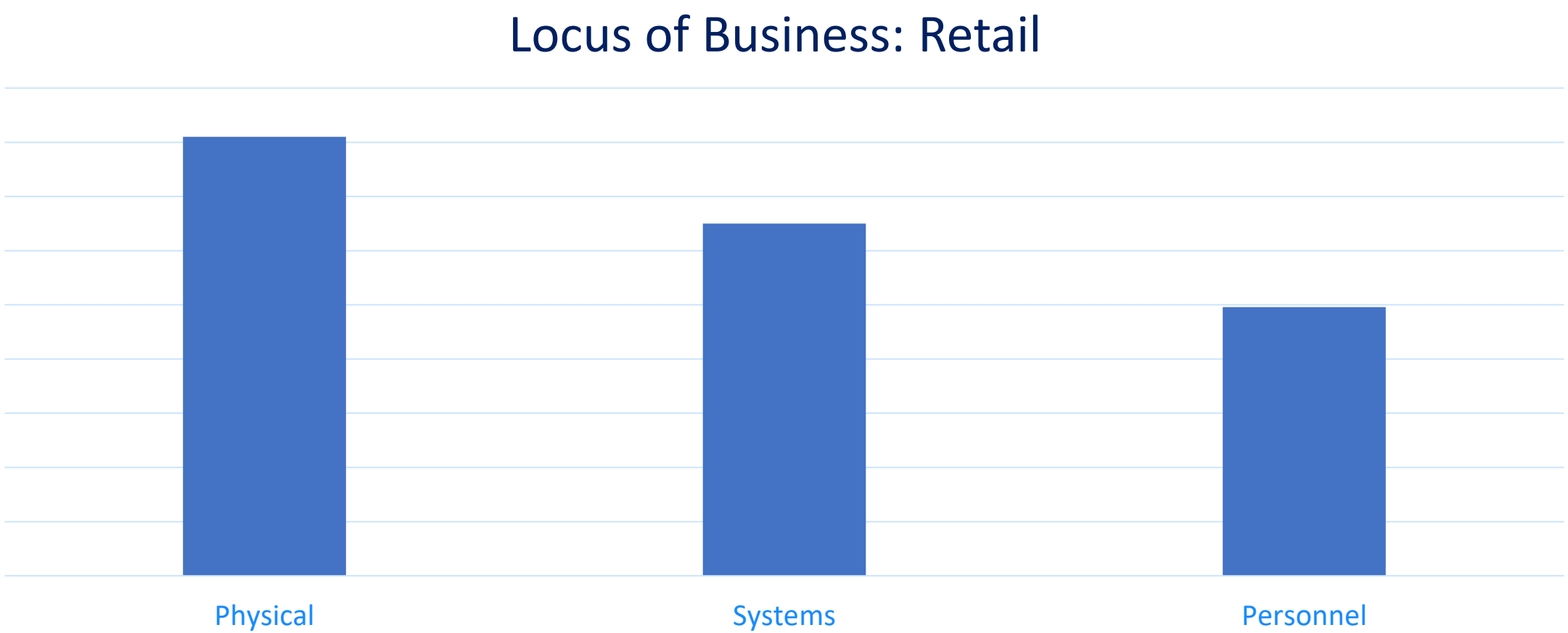
Know Your Business:
Where is Business Conducted/Business Assets?



Know Your Business:
Where is Business Conducted/Business Assets?



Know Your Business:
Where is Business Conducted/Business Assets?

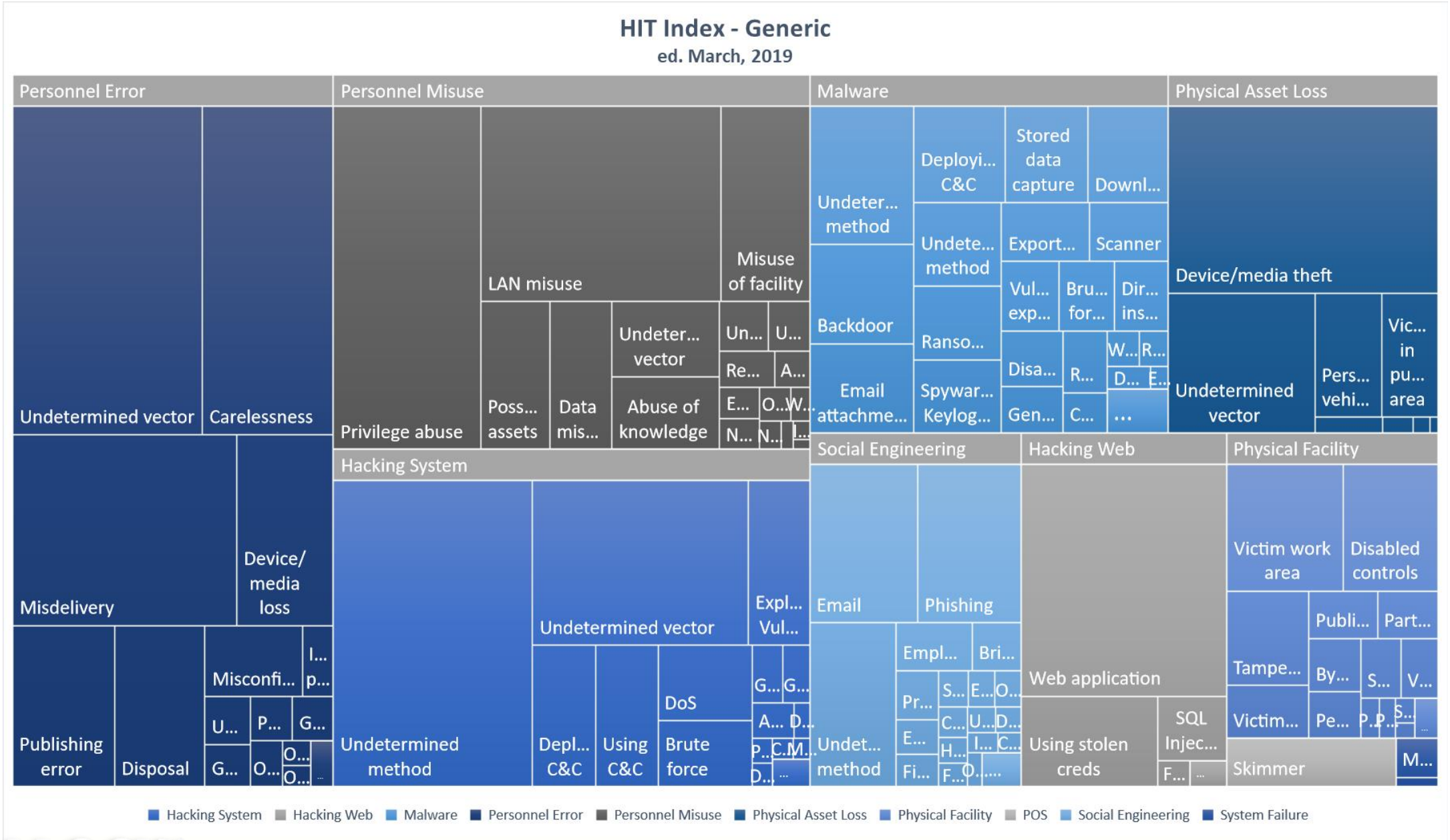


What Does the Data Teach Us?

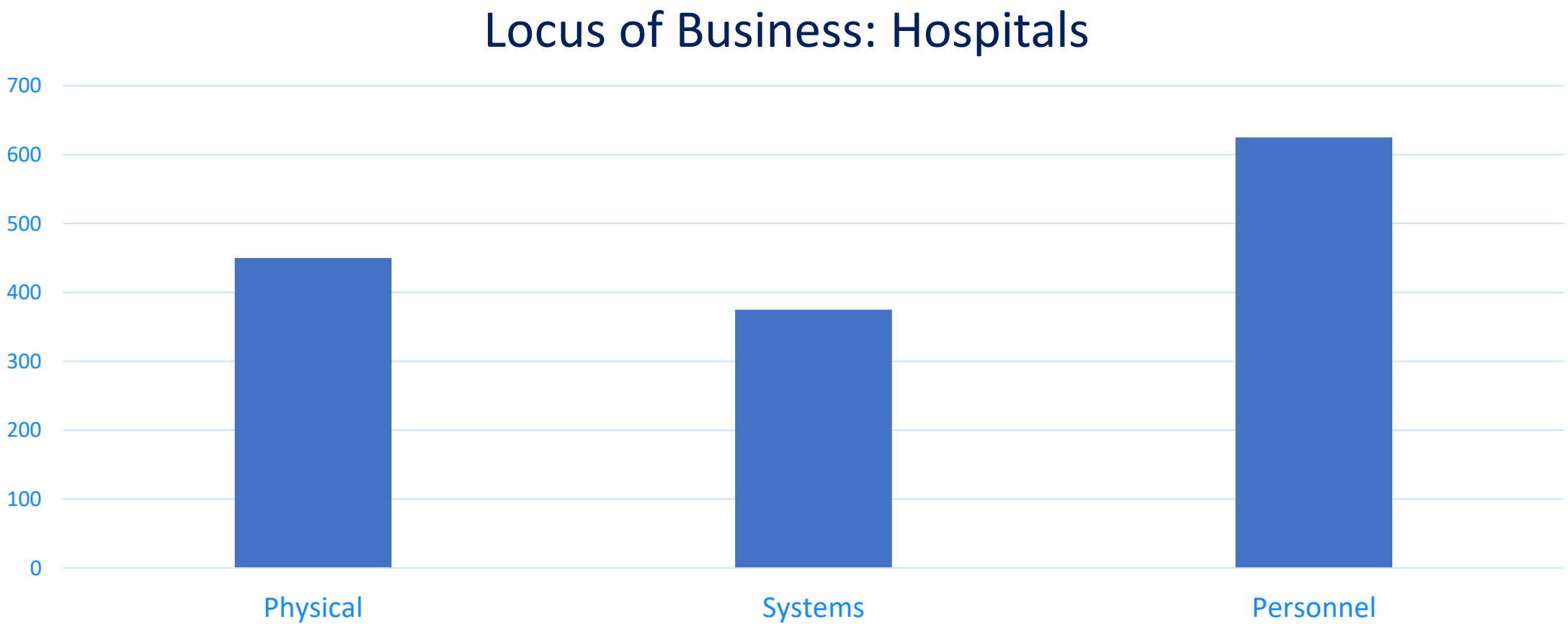
Your threat landscape is where you conduct business

So how do we forecast?

1. Know how your business operates
2. Know your threat landscape
3. Get threat data
4. Align threat data to your threat landscape
5. Organize data to see where threats *have been**

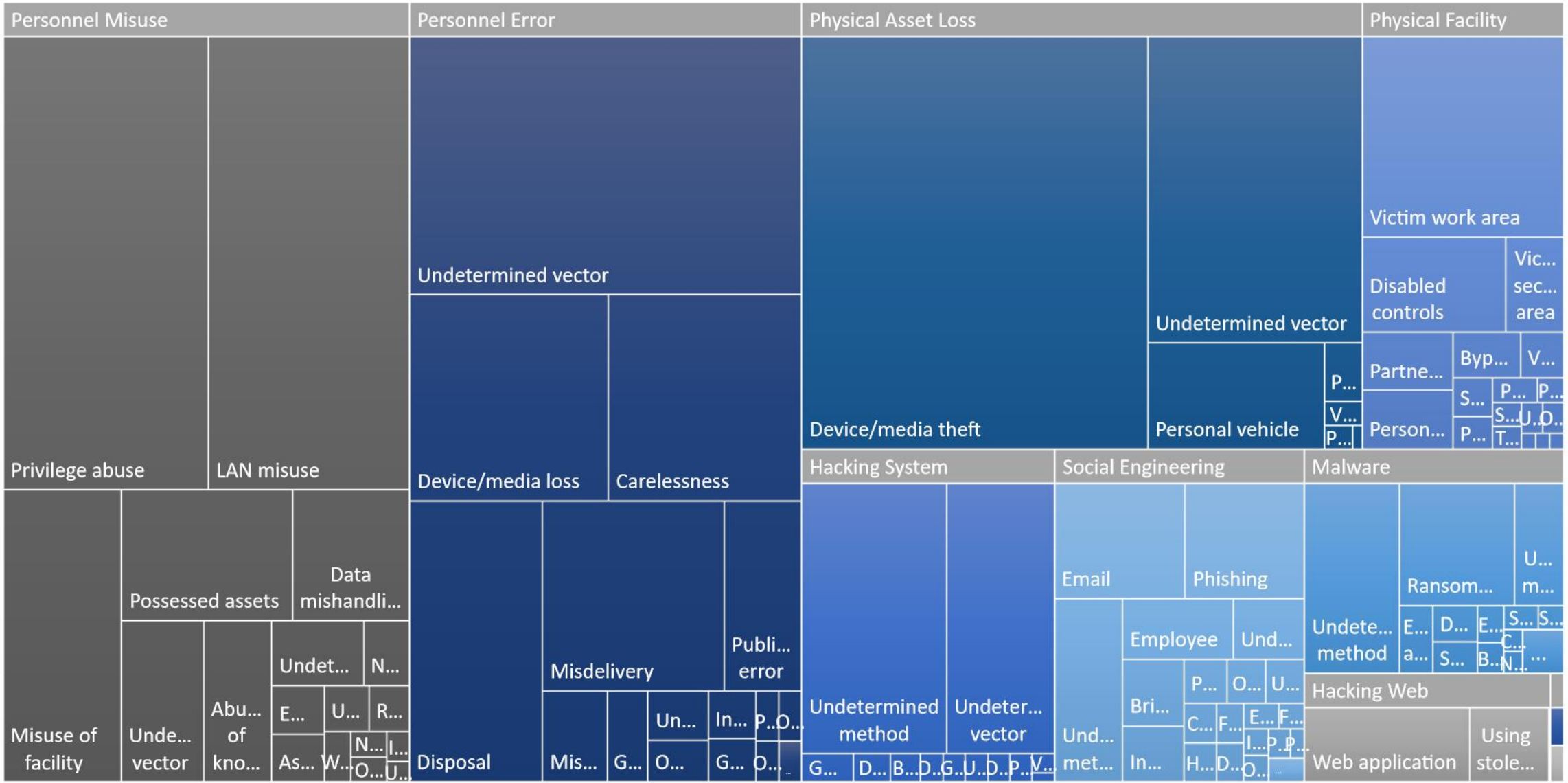

HIT Index - Generic
ed. March, 2019
Personnel Error
Undetermined vector
Carelessness
Misdelivery
Device/ media loss
Misconfi...
Publishing error
Disposal
Personnel Misuse
Privilege abuse
LAN misuse
Misuse of facility
Poss... assets
Data mis...
Undeter... vector
Abuse of knowledge
Malware
Undeter... method
Deployi... C&C
Stored data capture
Downl...
Backdoor
Undete... method
Export...
Scanner
Ranso...
Email attachme...
Spywar... Keylog...
Vul... exp...
Bru... for...
Dir... ins...
Disa...
R...
Gen...
C...
Physical Asset Loss
Device/media theft
Undetermined vector
Pers... vehi...
Vic... in pu... area
Hacking System
Undetermined method
Undetermined vector
Expl... Vul...
Depl... C&C
Using C&C
DoS
Brute force
Social Engineering
Email
Phishing
Undet... method
Empl...
Bri...
Hacking Web
Web application
Using stolen creds
SQL Injec...
Physical Facility
Victim work area
Disabled controls
Tampe...
Publi...
Part...
By...
S...
V...
Victim...
Pe...
Skimmer
Hacking System
Hacking Web
Malware
Personnel Error
Personnel Misuse
Physical Asset Loss
Physical Facility
POS
Social Engineering
System Failure

Data: Your Threat Landscape is Where Your Business is Conducted



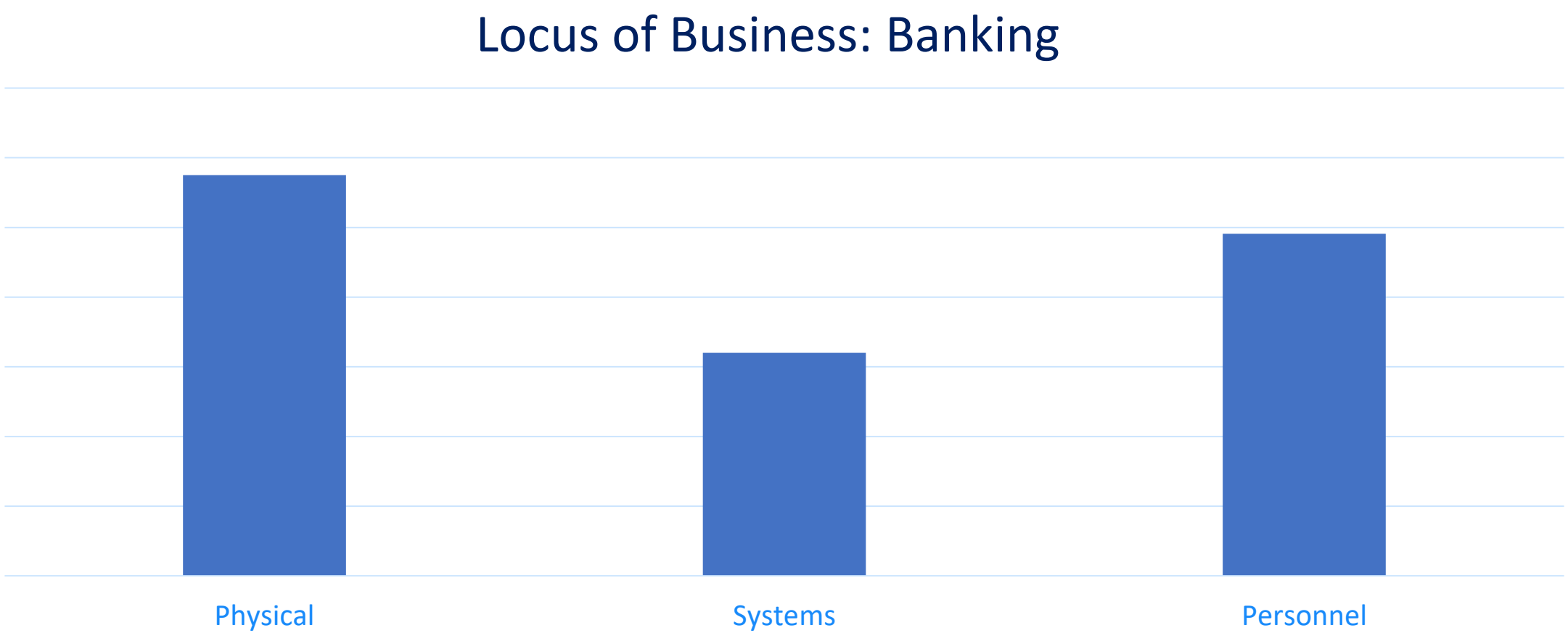
HIT Index - Clinical Healthcare

ed. March, 2019



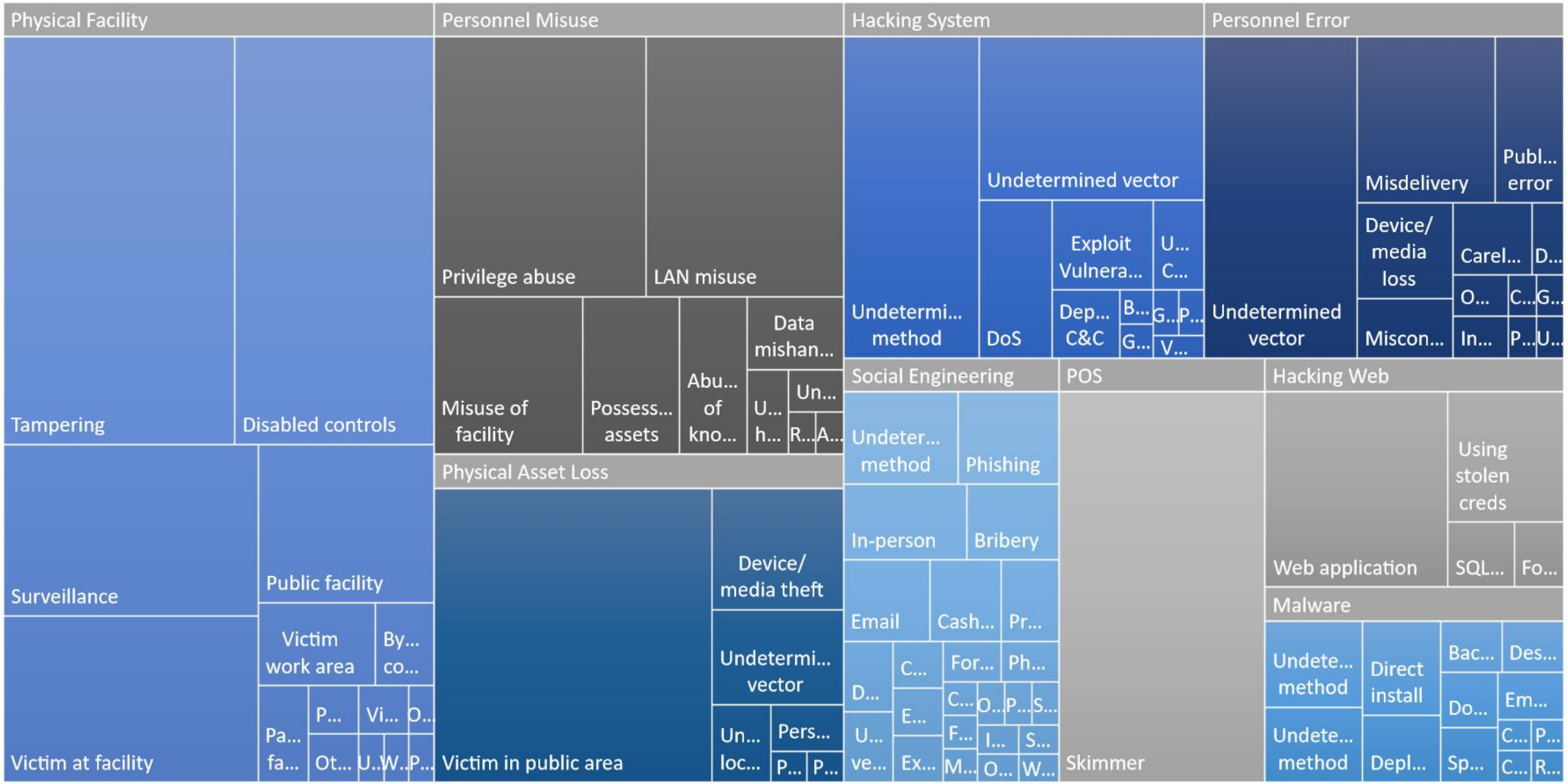
Hacking System · Hacking Web · Malware · Personnel Error · Personnel Misuse · Physical Asset Loss · Physical Facility · POS · Social Engineering · System Failure

Data: Your Threat Landscape is Where Your Business is Conducted

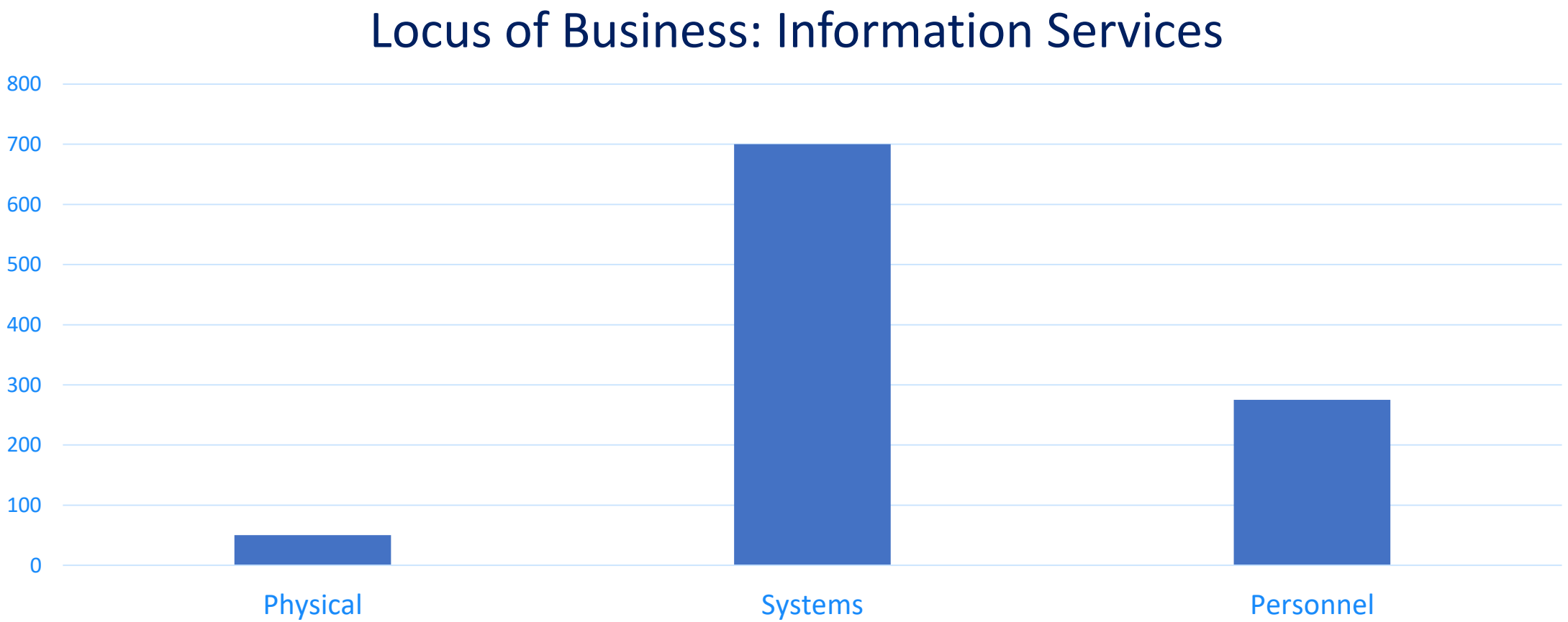


HIT Index - Retail Banking

ed. March 2019

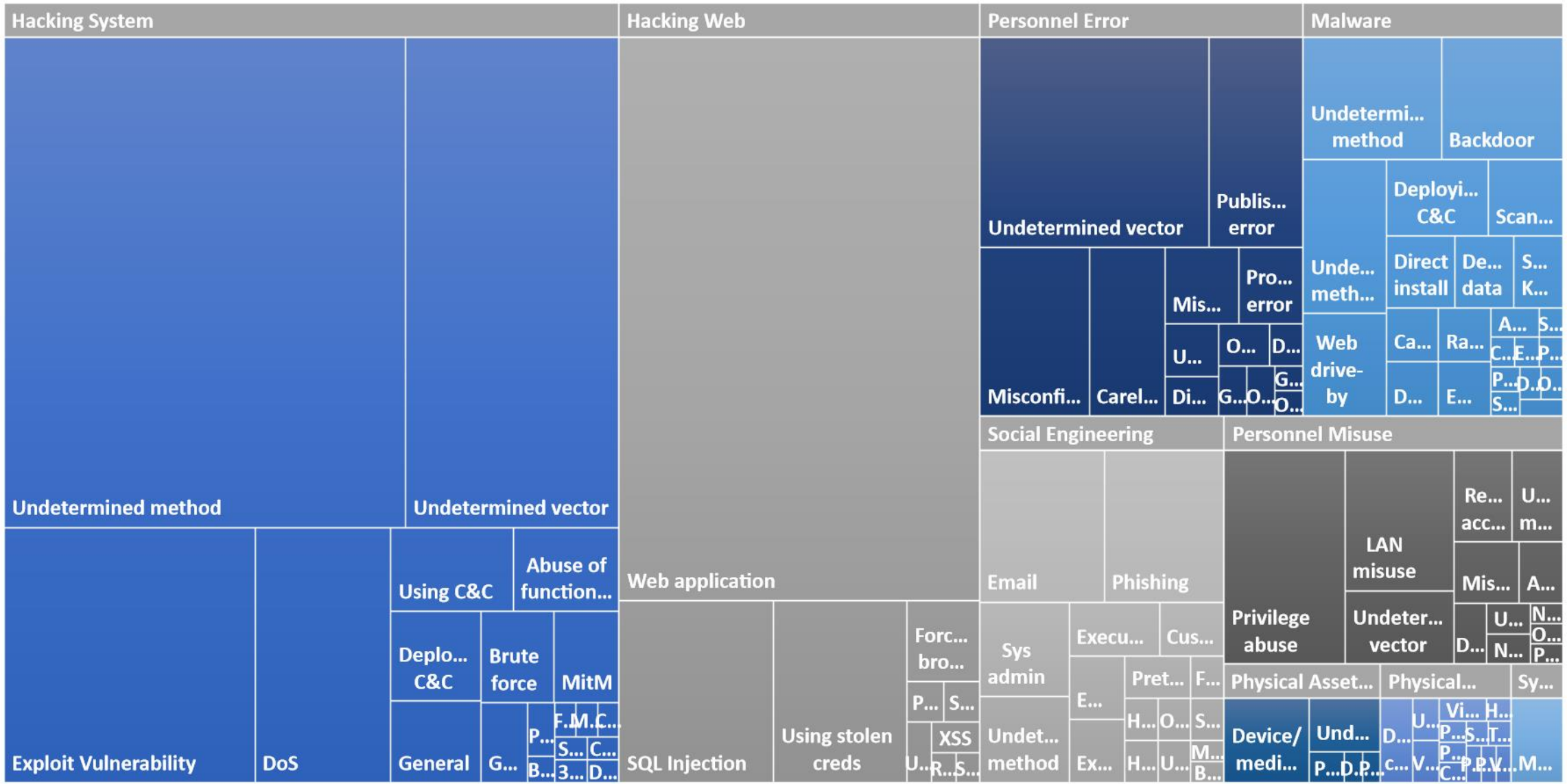


Data: Your Threat Landscape is Where Your Business is Conducted



HIT Index - Information Services

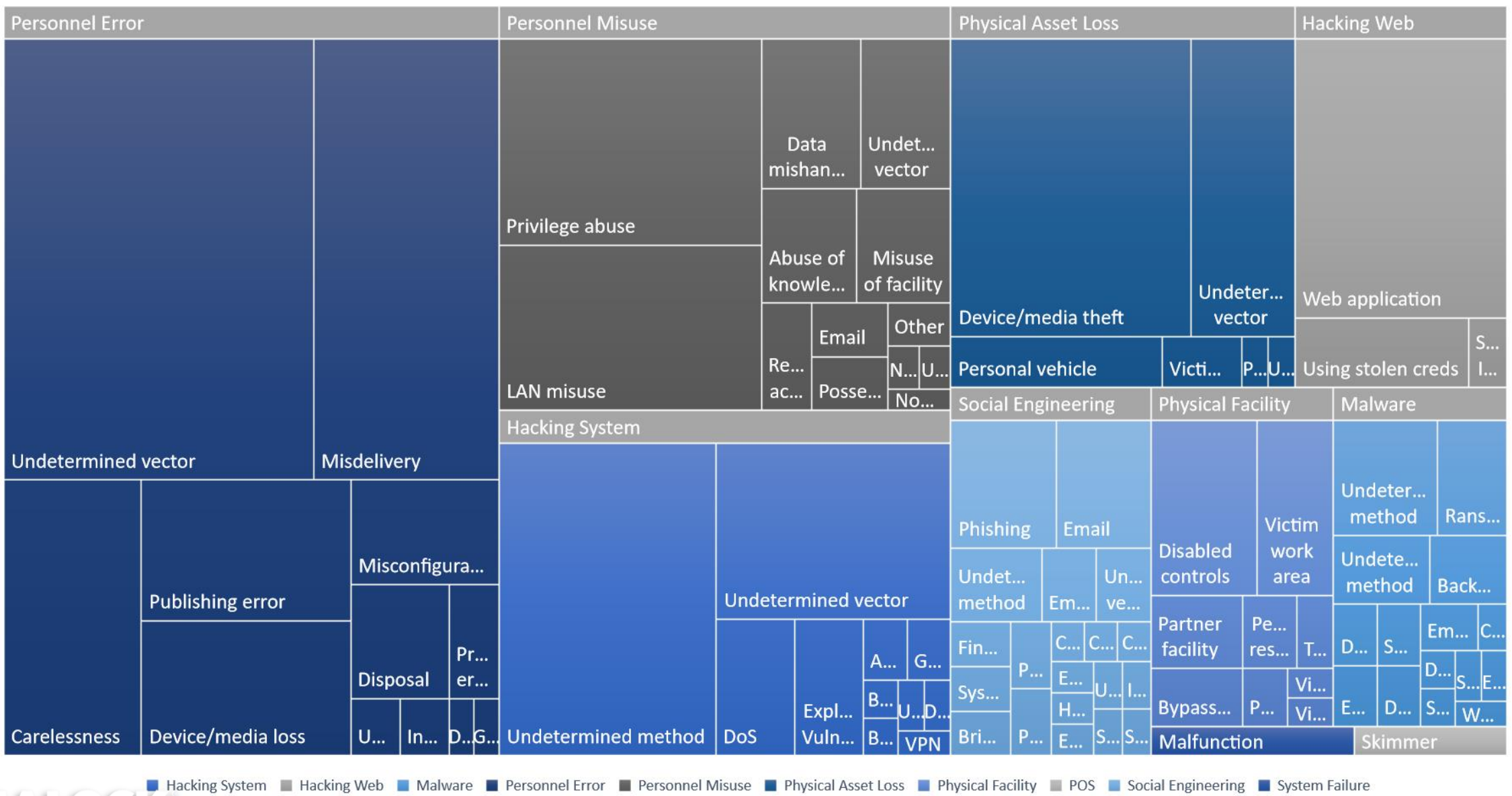
ed. March 2019



VCDB / HIT Index

- Financial services – Banking
- Financial services – Non-banking
- Education
- Public administration
- Professional services
- Clinical Healthcare
- Nonprofits
- Information services
- Retail
- Hospitality
- Manufacturing
- Etc …

Test the Hypothesis: What Business Is This?



Test the Hypothesis Results …

- Financial Advisors
  - Lots of 1-on-1 contact with customers
  - Most employees handling personal information
  - Lots of delivery and distribution of personal information
  - Rare on-site transactions

Past is Prologue

- Business Changes Slowly Enough that We Can Forecast Threat Landscapes by Watching What's Been Happening
  - Technical infrastructure
  - Go-to-market methods
  - Customer interaction "vectors"
  - Business processes
  - Reporting structures

So how do we forecast?

1. Know how your business operates
2. Know your threat landscape
3. Get threat data
4. Align threat data to your threat landscape
5. Organize data to see where threats *have been**

Veris Community Database (VCDB)

- Tremendously detailed look into ~9,000 reported incidents
- ~2,500 characterizations of incidents
- Sponsored by Verizon
  - Part of Annual DBIR
- Fed and maintained by a large community
- Records/details added regularly

Sources for Past Threats

- Technical Threats – *Good for tactical prep and response*
  - MISP
  - OpenCTI
  - CVE
  - Commercial vendors

- All Reported Threats – *Good for planning*
  - Veris Community Database
  - Privacy Rights Clearinghouse
  - Information Sharing and Analysis Centers (ISACs)

So how do we forecast?

1. Know how your business operates
2. Know your threat landscape
3. Get threat data
4. Align threat data to your threat landscape
5. Organize data to see where threats *have been**

Data Characteristics Found in VCDB

- Basic facts (who, what, when, where)
- Exploited assets (partial)
- Data classifications
- Nationality/location origin and target
- Third-party roles (partial)
- **Industries and sub-industries**
- **Threat actions**
- **Threat vectors**
- Size of breach ?
- Financial impacts ?
- …

Align threat data to your threat landscape

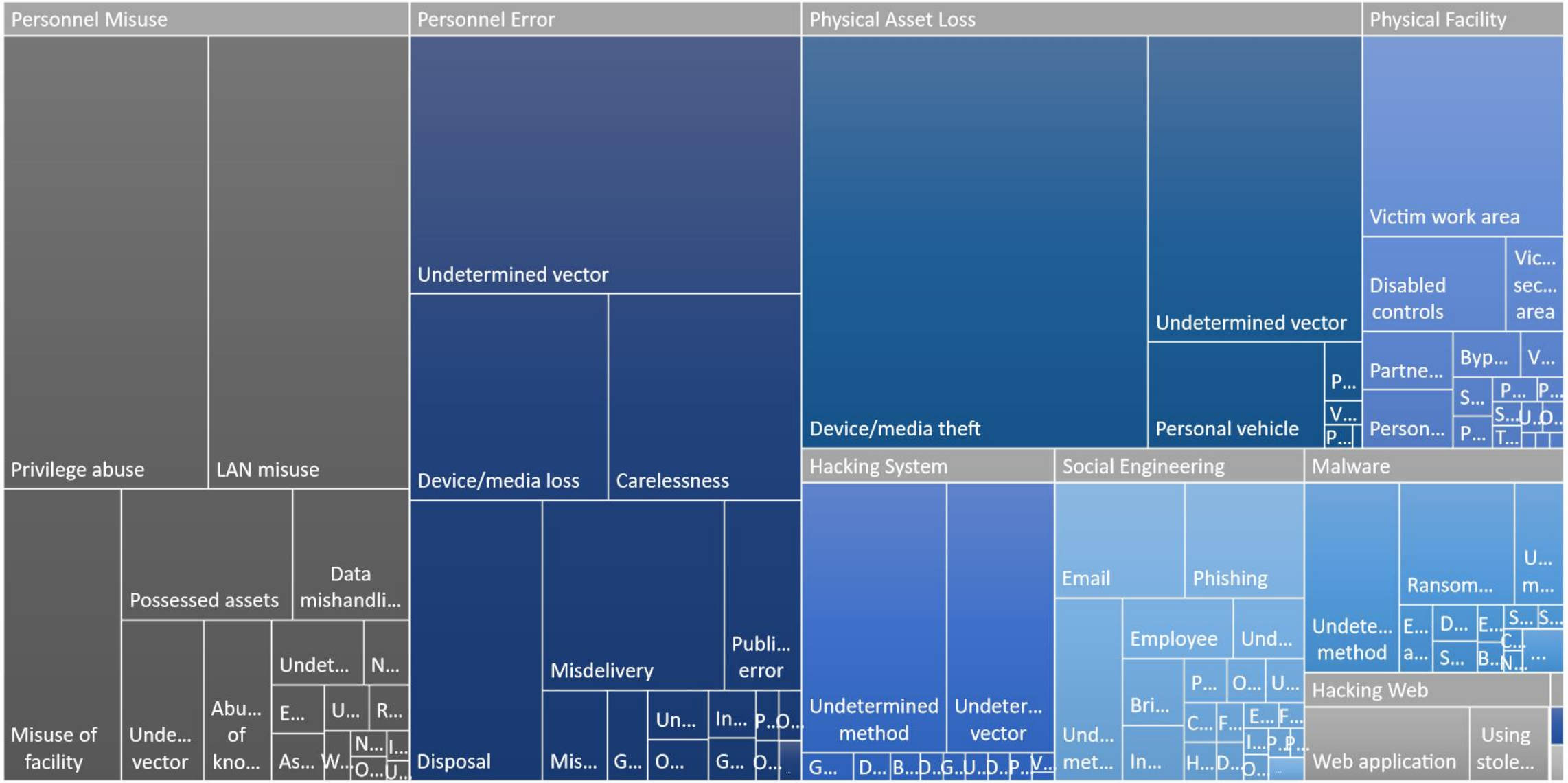
- How your business functions (industry class)
- What you can manage (threats)

So how do we forecast?

1. Know how your business operates
2. Know your threat landscape
3. Get threat data
4. Align threat data to your threat landscape
5. Organize data to see where threats have been*

HIT Index - Clinical Healthcare

ed. March, 2019



Hacking System Hacking Web Malware Personnel Error Personnel Misuse Physical Asset Loss Physical Facility POS Social Engineering System Failure

Past is Prologue

- Yes, cyber threats change often. But *generally* within the same threat landscape.
  - Business changes slowly enough to forecast threats landscapes
- *“I thought these threats were foreseeable, because they are frequently reported as threats in organizations like mine.”*
- *“I thought these other threats were unlikely because they are so rarely reported as threats in organizations like mine.”*

What About COVID 19?

That’s where your risk assessment will come in ...

How to Use Threat Forecasting in Risk Assessments

What Risk Assessments *Are* …

Estimation of Likelihood and Impact of Bad Events

- How likely is it that bad things will happen?
- What's the harm when they do happen?

May be Qualitative or Quantitative

- "Many residents will likely get sick and very few may die …"
- "170 – 426 students will suffer 3.4% - 51.7% temporary health detriment. .1% - .6% may die."

What Risk Assessments *Are NOT* …

Audits, Gap Assessments, or Scans

- “Here’s your vulnerabilities!”

Maturity Assessments

- “You rate a ‘2.1’ out of ‘5’”
- “You should get to ‘3’. That’s where your peers are.”

Maturity Scoring (example)

Maturity Score	Meaning
1	Ad hoc / not implemented
2	Documented / Inconsistent
3	Implemented Consistently
4	Tested and Corrected
5	Innovative or Root Cause

Consultants' "Goal"

Typical Regulations

ISO 27001, et al

Duty of Care Risk Analysis

Impact *(Others)* **x Likelihood**

Impact *(You)* **x Likelihood**

Recent Law

- **7.1 As part of the Information Security Program, Orbitz, Expedia shall include risk management, which at a minimum includes:**

  a. Documented criteria for reasonable safeguards that appropriately protect Consumers while not being more burdensome to Orbitz than the risks they address. These criteria shall include:

    i. Obligations owed to the Consumers for protecting their Personal Information,

    ii. The social utility of Orbitz's handling of Consumers' Personal Information,

    iii. The foreseeability and magnitude of harm caused by security threats,

    iv. The burden of Orbitz's utility and objectives posed by safeguards,

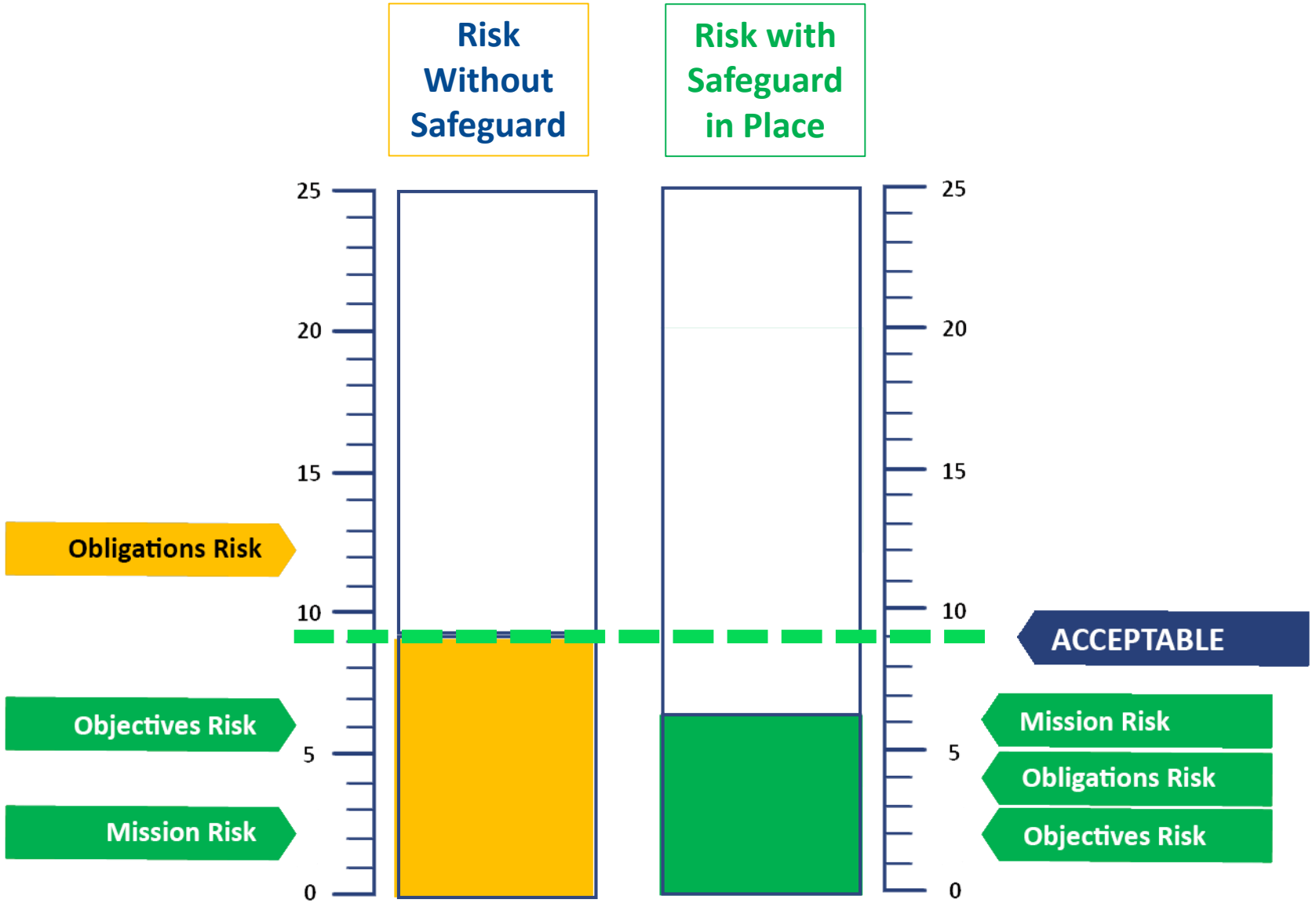
    v. The overall public interest in the proposed solution.

**Commonwealth of Pennsylvania v Expedia and Orbitz, December, 2019*

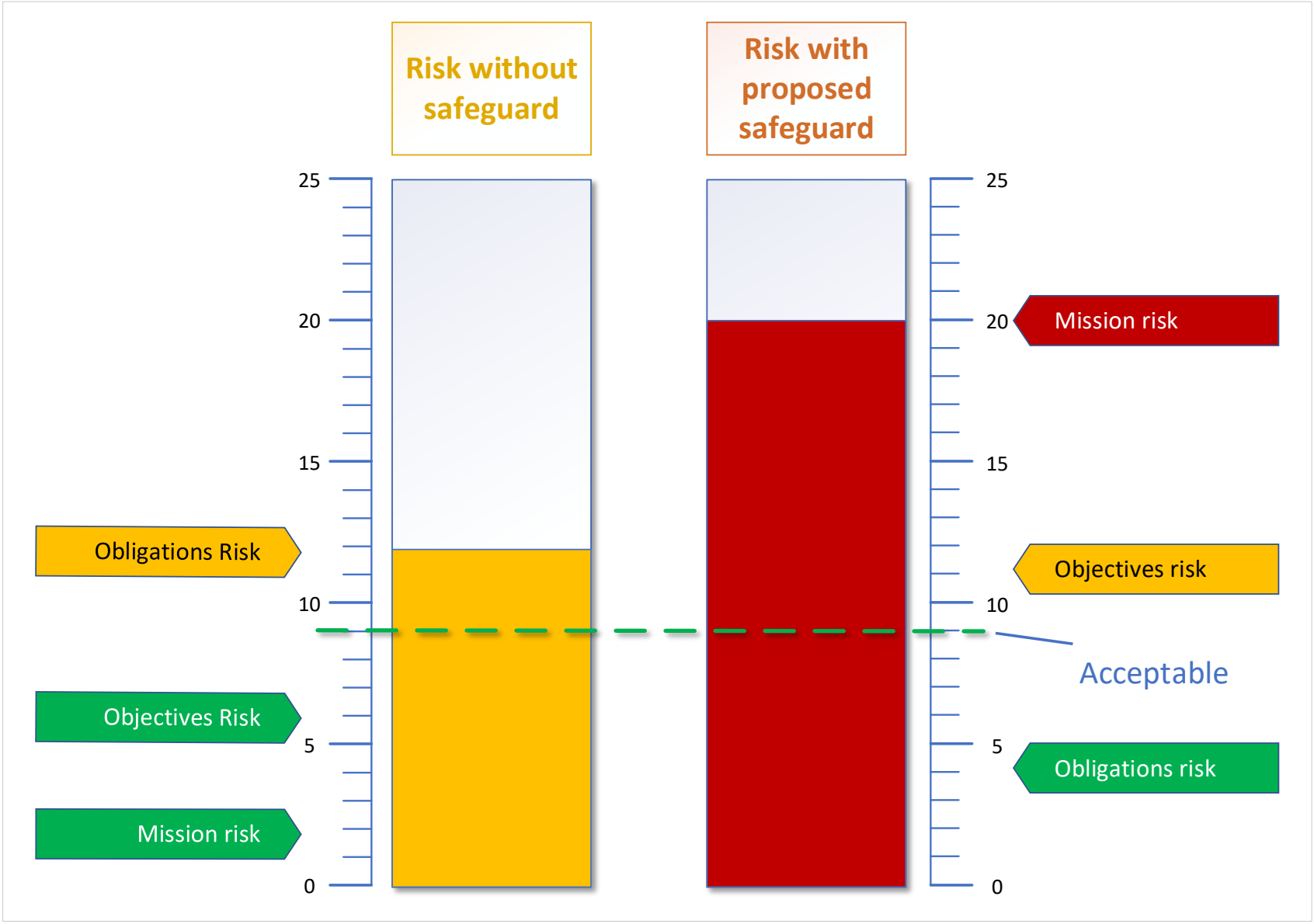
Duty of Care Risk Analysis at its Simplest

Neither your conduct, nor your controls, may create a likelihood of harm (to yourself or others) large enough to require correction.

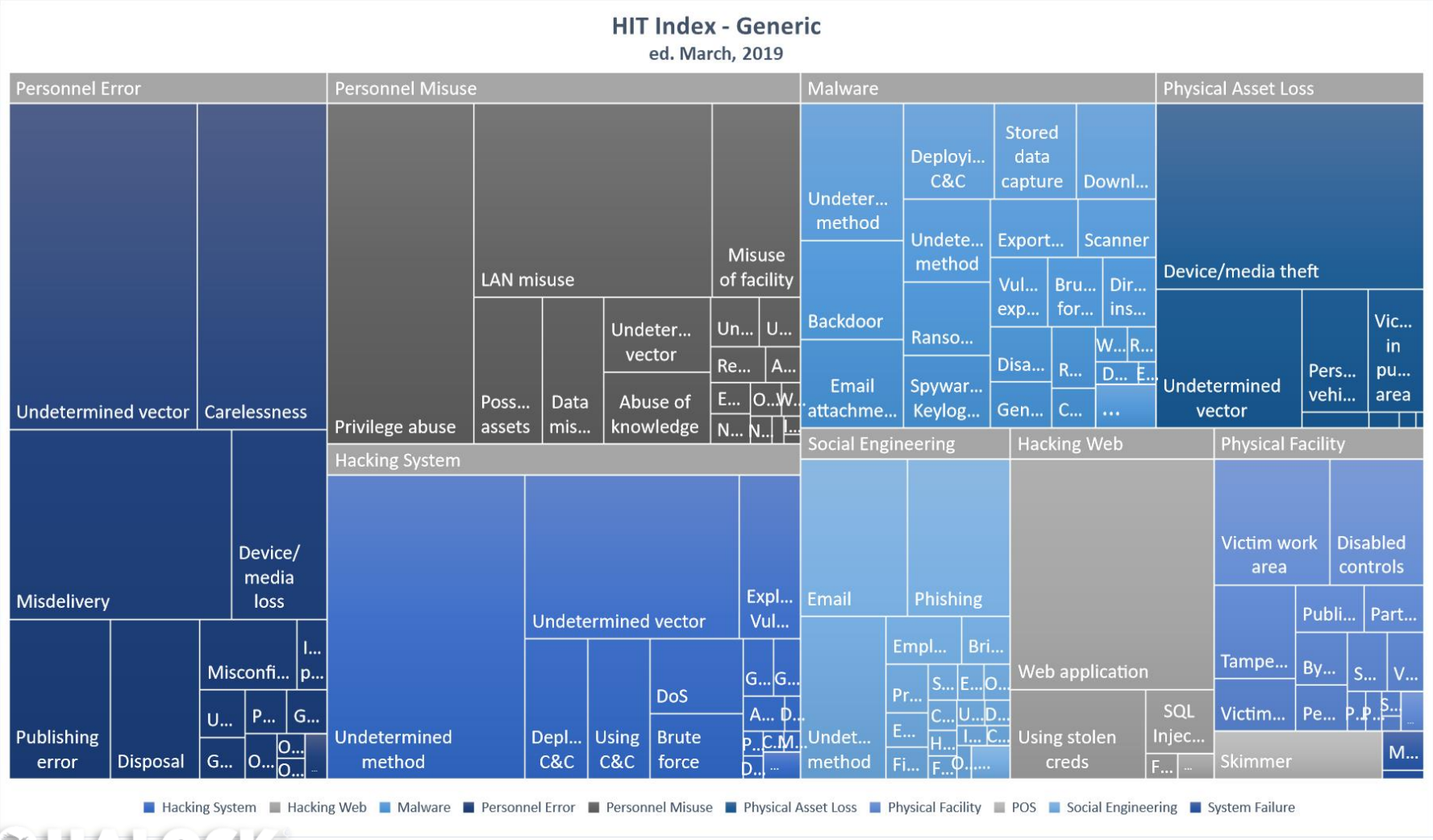
How do I know if a Control is Reasonable?



This safeguard is NOT reasonable.



Using Foreseeability in Risk Analysis



Threat Clusters	Count	Percentage
Personnel Error	4748	58%
Personnel Misuse	3710	45%
Hacking System	3341	41%
Malware	2662	32%
Physical Asset Loss	2011	25%
Social Engineering	1553	19%
Hacking Web	1506	18%
Physical Facility	1344	16%
POS	170	2%
System Failure	42	1%

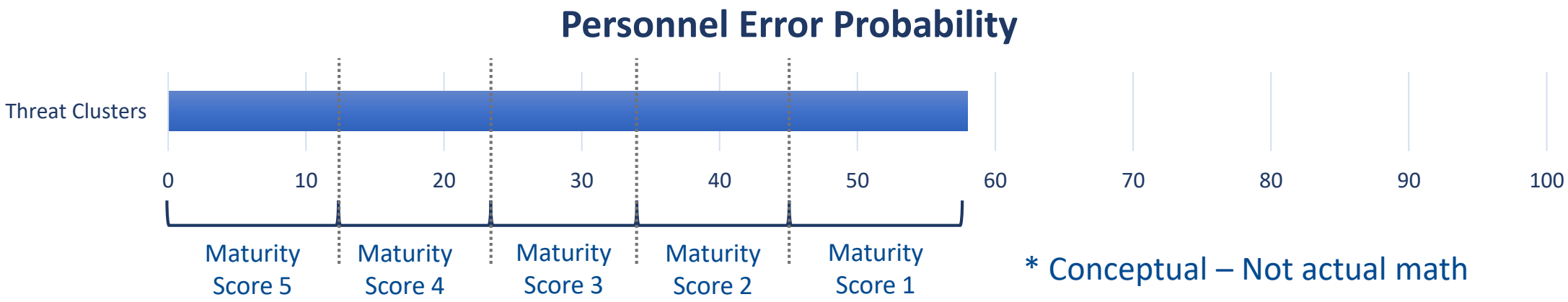
Likelihood = Forecast – Control Strength

Threat Clusters	Percentage
Personnel Error	58%
Personnel Misuse	45%
Hacking System	41%
Malware	32%
Physical Asset Loss	25%
Social Engineering	19%
Hacking Web	18%
Physical Facility	16%
POS	2%
System Failure	1%

vs.

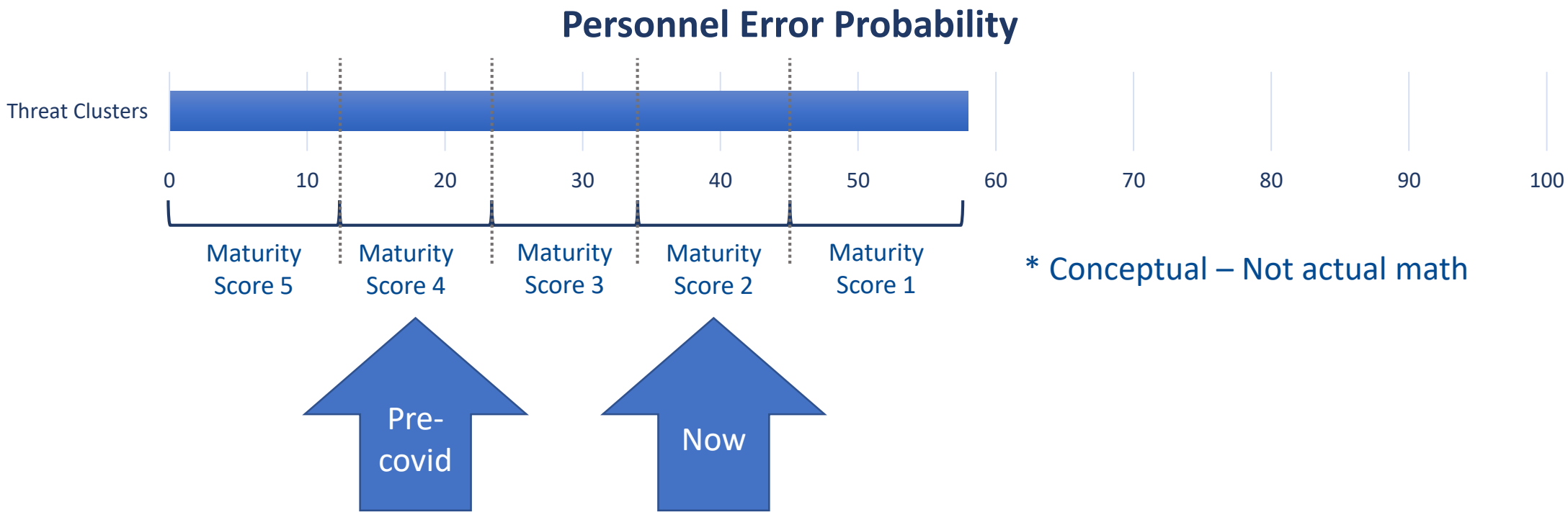
Control Maturity	Meaning
1	Ad hoc / not implemented
2	Documented / Inconsistent
3	Implemented
4	Tested and Corrected
5	Innovative or Root Cause

Mitigate the Forecast by the Strength of Controls



* Conceptual – Not actual math

Mitigate the Forecast by the Strength of *Changing* Controls



* Conceptual – Not actual math

Mitigate the Commonality by the Strength of Controls

Quintile % Threat	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Maturity of Control	1	1	1	1	1	2	2	2	2	2	3	3	3	3	3	4	4	4	4	4	5	5	5	5	5
Likelihood	**3**	**4**	**4**	**5**	**5**	**2**	**3**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**3**	**4**	**1**	**1**	**2**	**2**	**3**

* Conceptual – Not actual math

Your threat landscape is where your business is conducted

Thank You

Chris Cronin

HALOCK Security Labs

ccronin@halock.com

HALOCK®