Did you accept the risk?

Dynamic risk metrics in your environment.

SnykCon 2020

DATADOG

a.k.a. The Safety Dance

You can dance if you want to—but you can’t leave risk behind.

SnykCon 2020

DATADOG

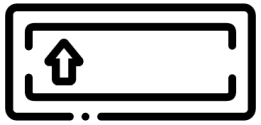
Your Safety Dancers for today

Andrew Krug

Daniel Maher

DATADOG

The dance card

- Risk management (a classic!)
- Real-world risk analysis (explosions!)
- Risk in the context information technology (`cyber`!)
- Virtual-world risk analysis (routing tables!)
- How to shift-left to avoid specific risks ( !)
- Walk through a sample application (dance party!)

Crash Course in Risk
Risk 101

What is risk? What is safety science?
Classic calculation

$$R = f(s, p, c)$$

Risk = *f* (scenario, probability, consequence)

What is risk? What is safety science?
Kaplan and Garrick (1989)

What can go wrong?

What is the likelihood? (probability)

How bad could it be?

Qualitative vs Quantitative

Qualitative reasoning *ranks* likelihood using a scale score metric.

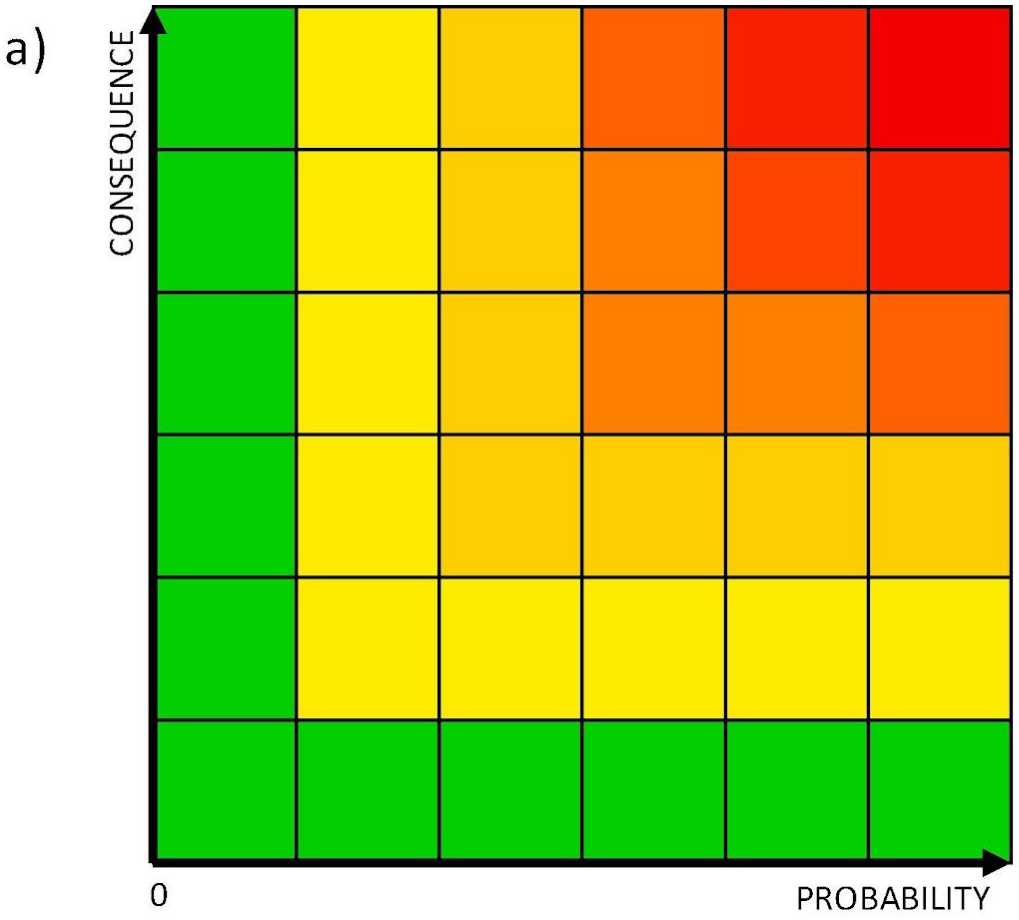
👍	👎
Speedy Easy Light data gathering!	Light data gathering? Low precision

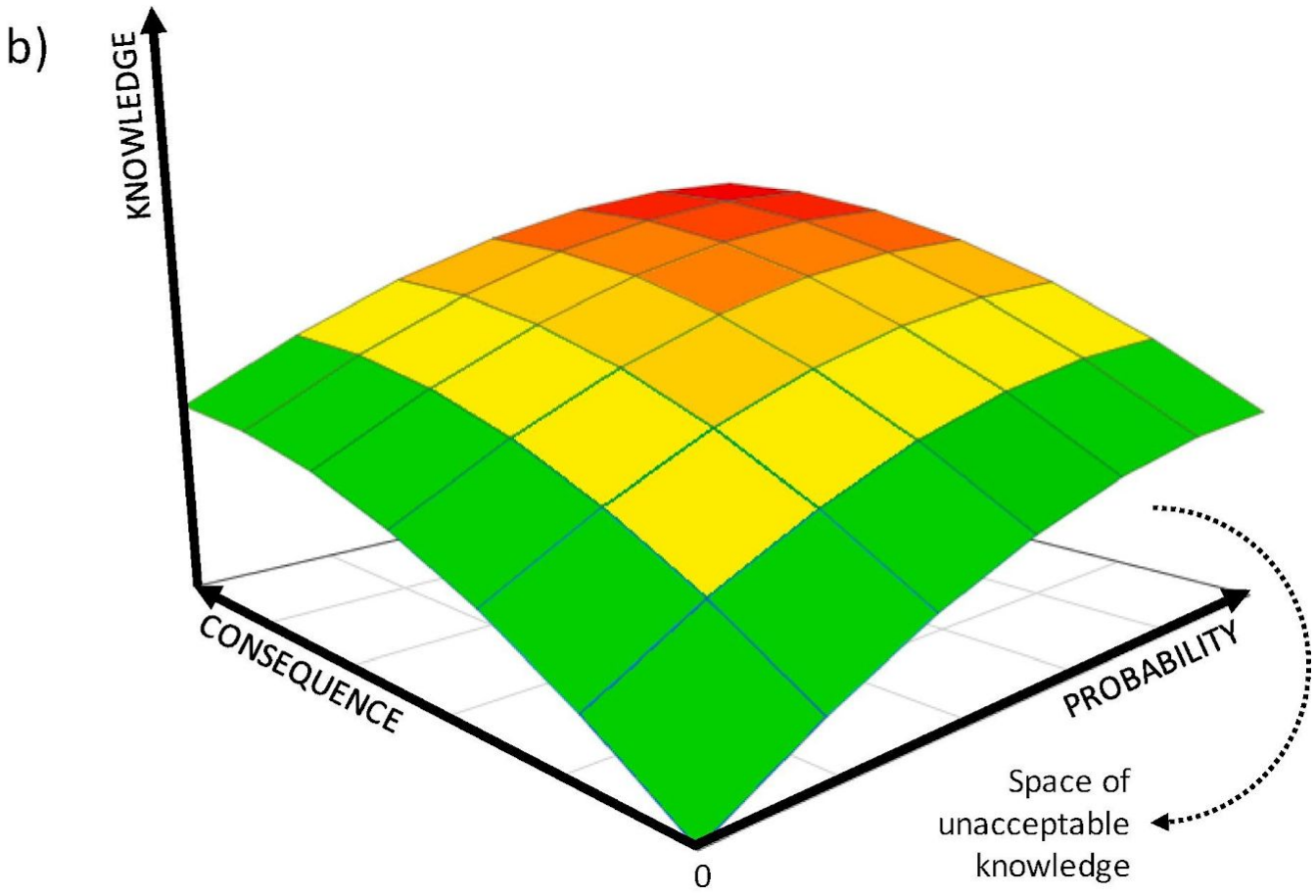
Qualitative vs Quantitative

Quantitative reasoning uses data to *reason* about probabilities and consequences.

👍	👎
Accuracy	Time Data Relative risks (adjacent)

Hybrid Models





T. Aven, "Three influential risk foundation papers from the 80s and 90s: Are they still state-of-the-art?," *Reliability Engineering & System Safety*, 28-Sep-2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832019302649?via=ihub. [Accessed: 15-Oct-2020].

What is risk? What is safety science?
Hybrid calculation

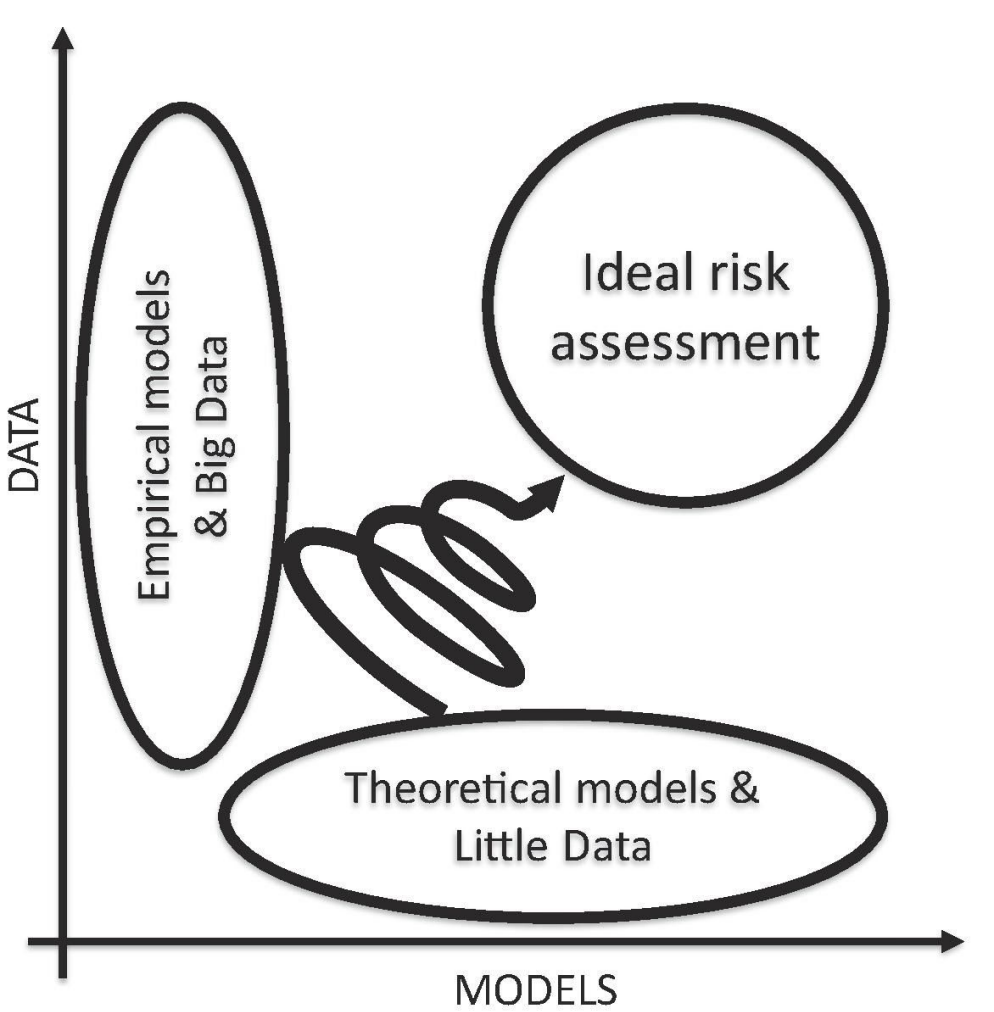
$$R = f(s, p, c, k)$$

Risk = *f*(scenario, probability, consequence, knowledge)

knowledge = (mix of both quantitative and qualitative data)

Risk analysis in the real world

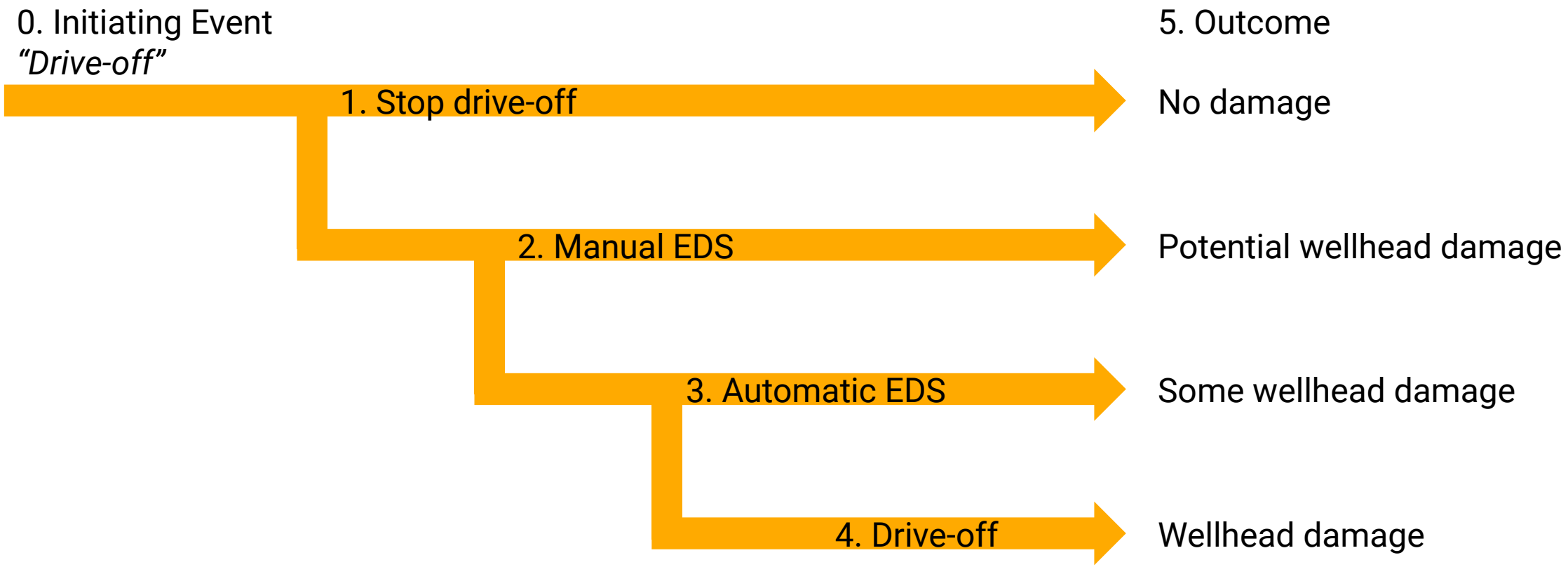
Real-world risk analysis
Industrial Modeling



T. Aven, “Three influential risk foundation papers from the 80s and 90s: Are they still state-of-the-art?,” *Reliability Engineering & System Safety*, 28-Sep-2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0951832019302649?via=ihub. [Accessed: 15-Oct-2020].

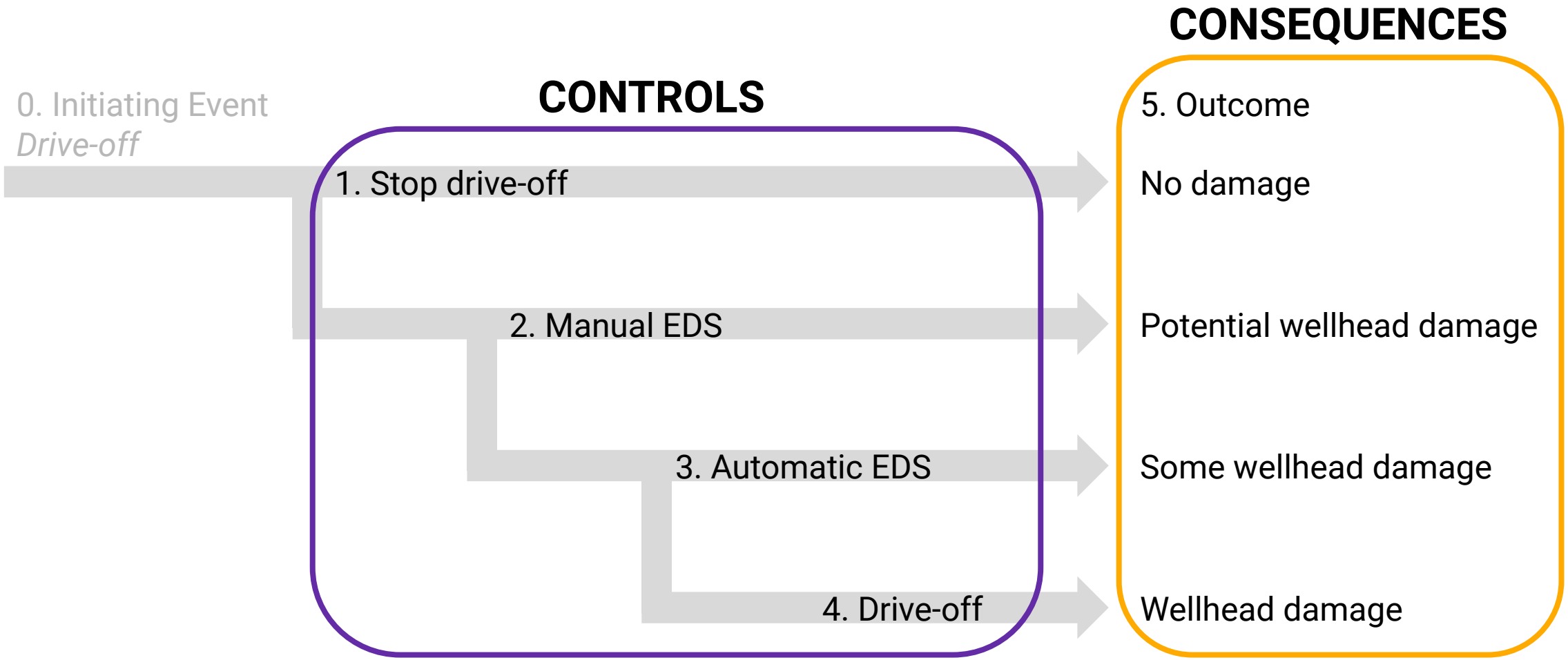
DATADOG

Real-world risk analysis
Oil Drilling



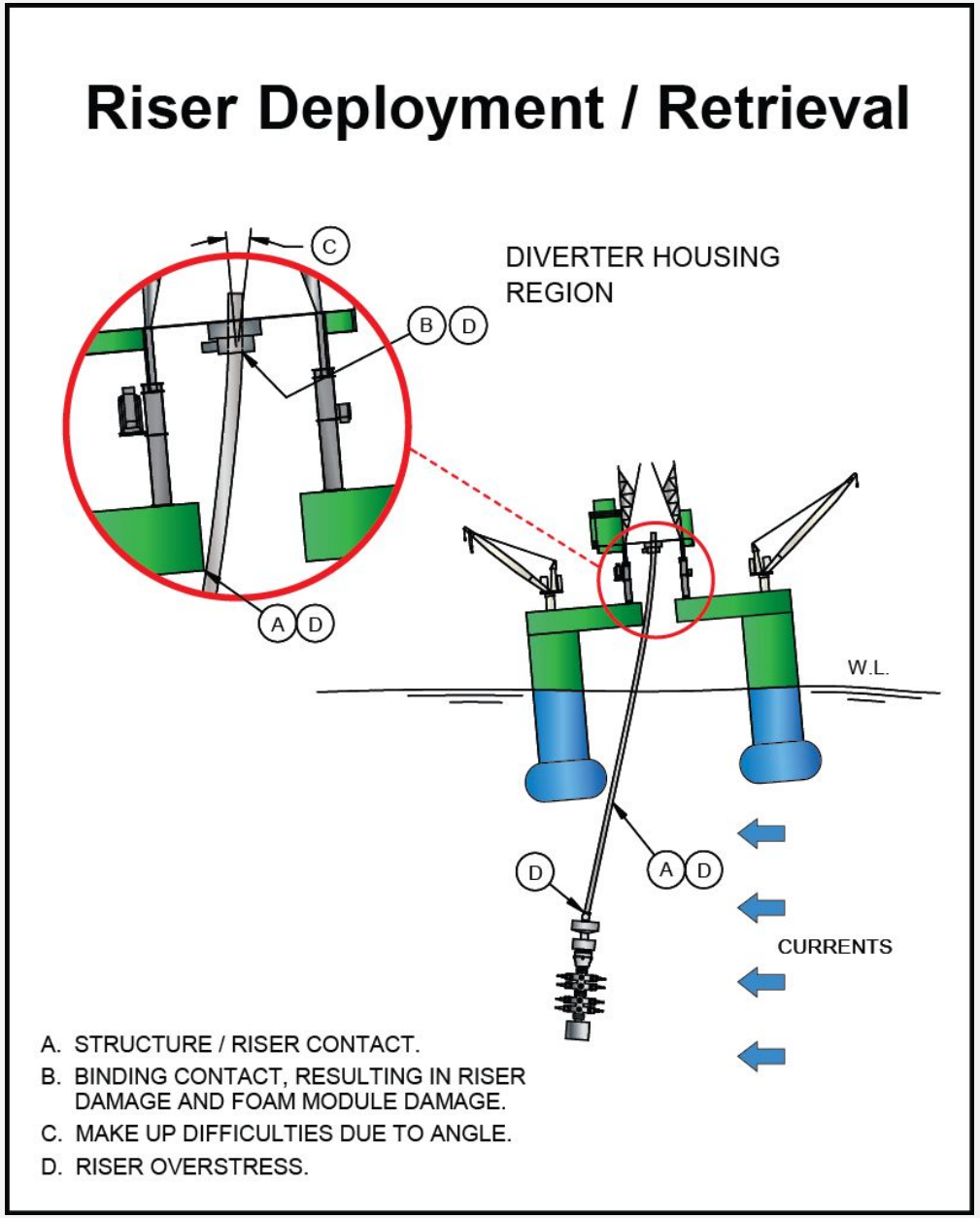
DATADOG

Real-world risk analysis
Oil Drilling



DATADOG

Pictures = 1000x words



S. E. Services, Inc., “Offshore Drilling Design & Analysis: Stress Engineering,” *Offshore Drilling Analysis Testing*, 2020. [Online]. Available: https://www.stress.com/capabilities/upstream/offshore-drilling [Accessed: 15-Oct-2020].

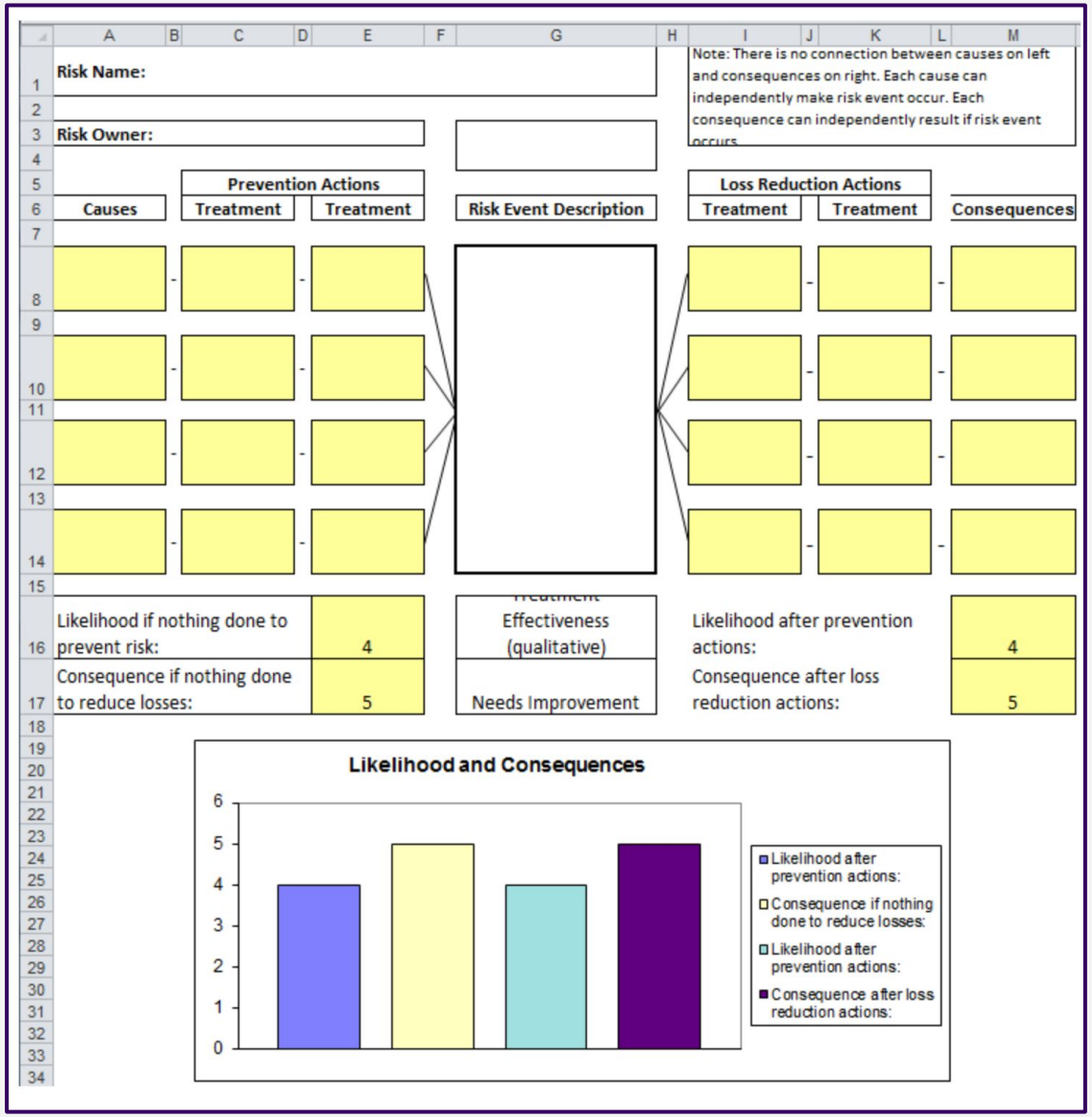
Bowtie Model (Hybrid)

Purpose

Developed to reason about known and unknown risks where the impact is *extremely* high (ex. loss of life).

What's new?

Describes control impacts on risk over time.



DATADOG

Risk in operations, development, and cyber security

Risk as it relates to operations

Risk	Impact	Likelihood
The site is down	No sales	Maybe?
	Front page of the orange site	*Strong maybe* because metrics?
	Wake. Up. EVERYONE.	97p based on uptime over the past two years…

DATADOG

Risk as it relates to development

Risk	Impact	Likelihood
Failed feature release	Time to rollback Reputation Lost revenues	How often?
Dropped sessions	Lost revenue Troubleshooting Bugfix	How much test coverage?
UI Bugs	Reputation Bugfix	How much frontend testing?

DATADOG

Risk as it relates to cyber security

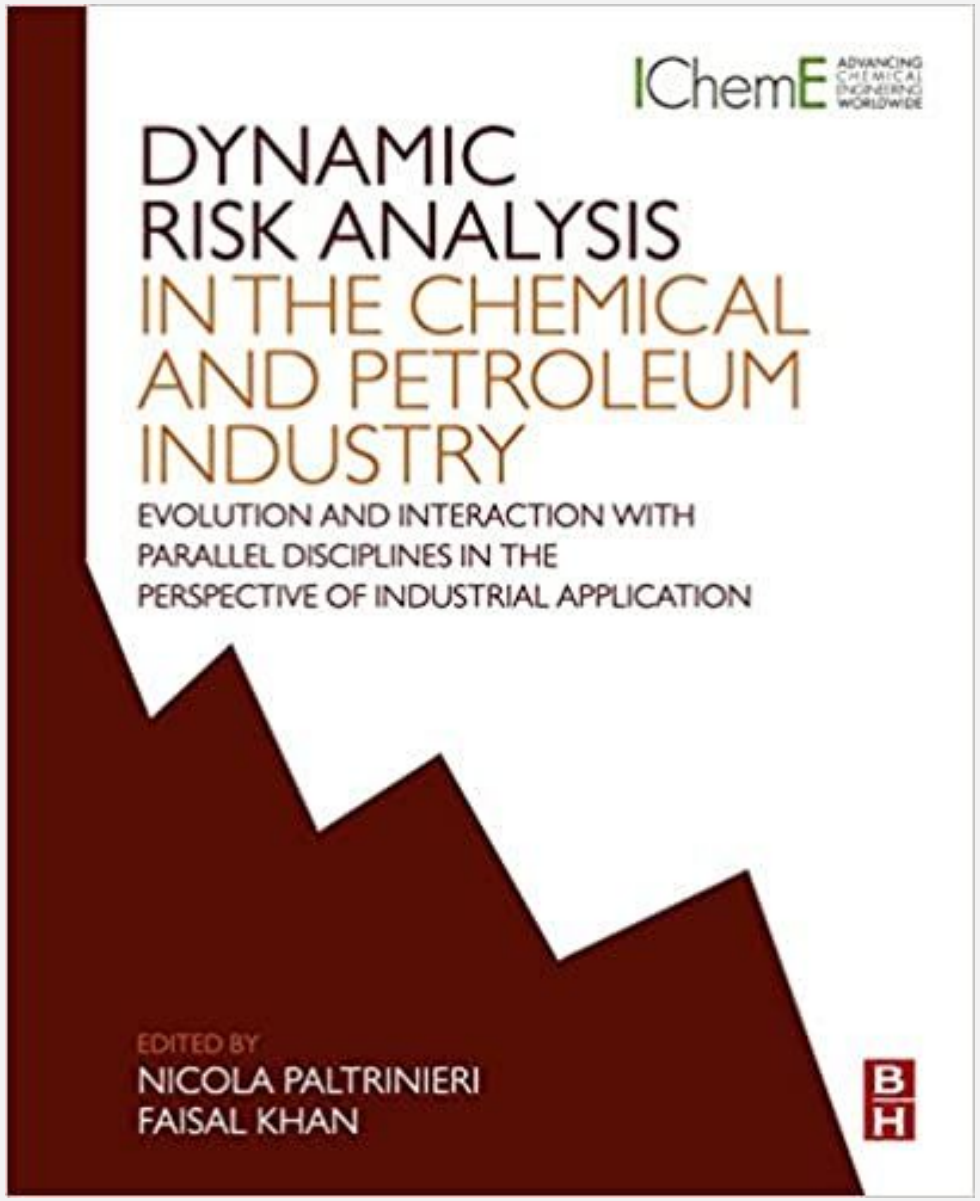
Risk	Impact	Likelihood
Supply chain vulnerability	Time to patch Firefighting Panic	?
SQL injection	Damage to reputation	? ?
XSS	User data theft Fines Lawsuits	? ? ?

DATADOG

Parallels to oil drilling

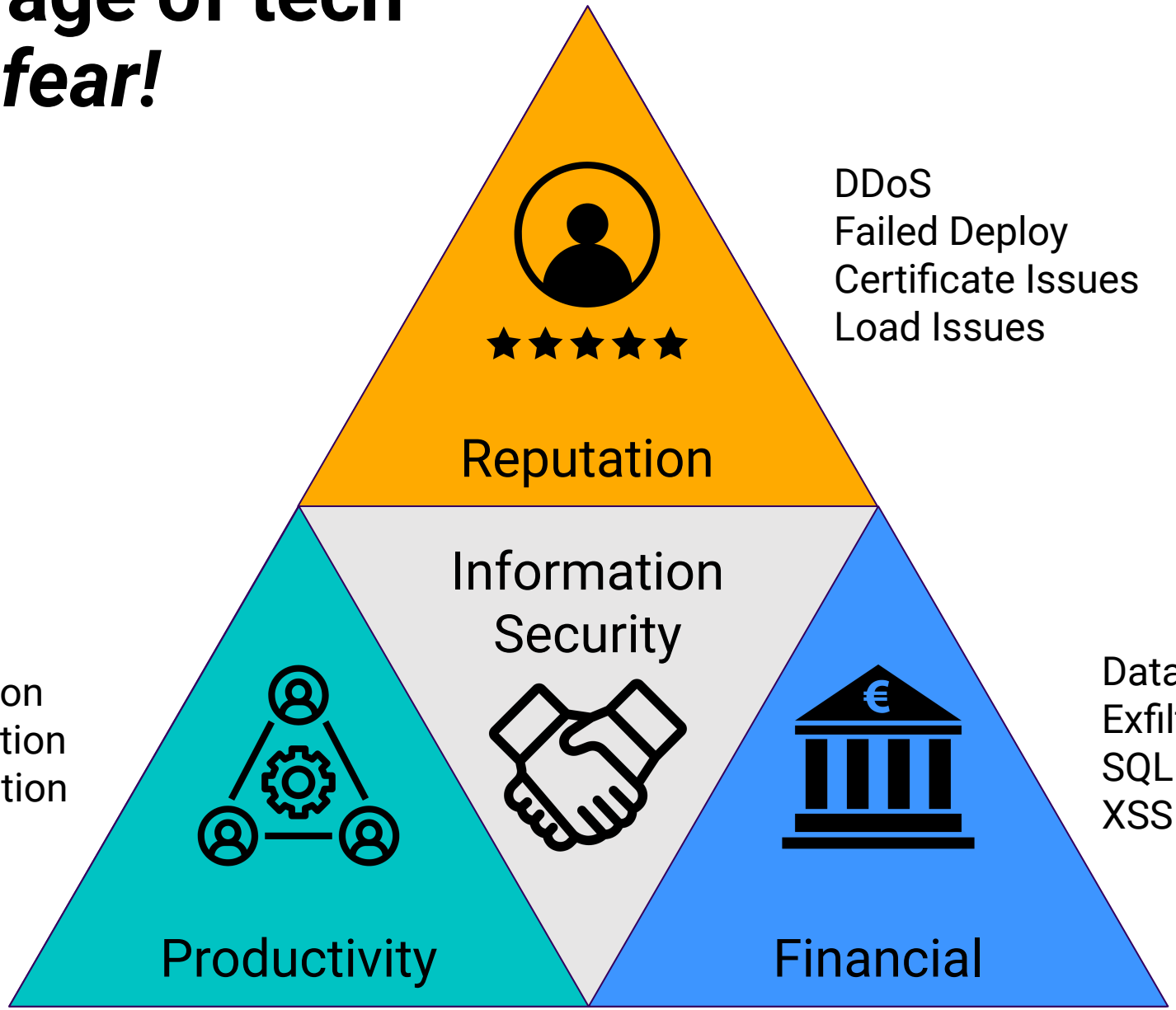
"[A]ccount for issues of human/machine interface, stress, shortage of time, and rare-event experience, which may lead the operator into failure and increase the probability of an accident."

— Nicola Paltrinieri (1996)



Examples of risk in the context of information technology

Risk in the age of tech
Triforce of fear!



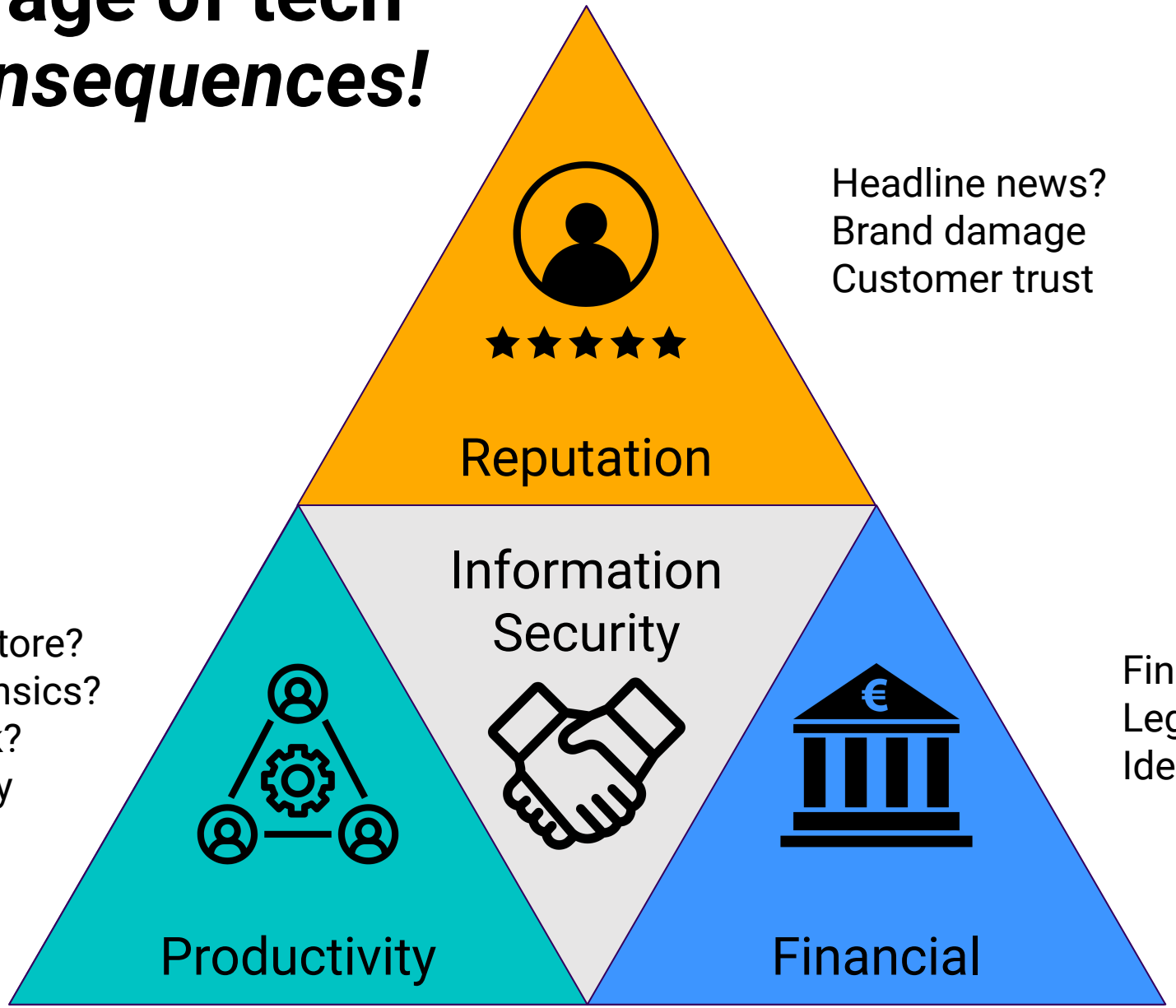
DDoS
Failed Deploy
Certificate Issues
Load Issues

Tampering
SQL Injection
Impersonation
Authentication
Bypass

Data
Exfiltration
SQL Injection
XSS

DATADOG

Risk in the age of tech
Triad of consequences!



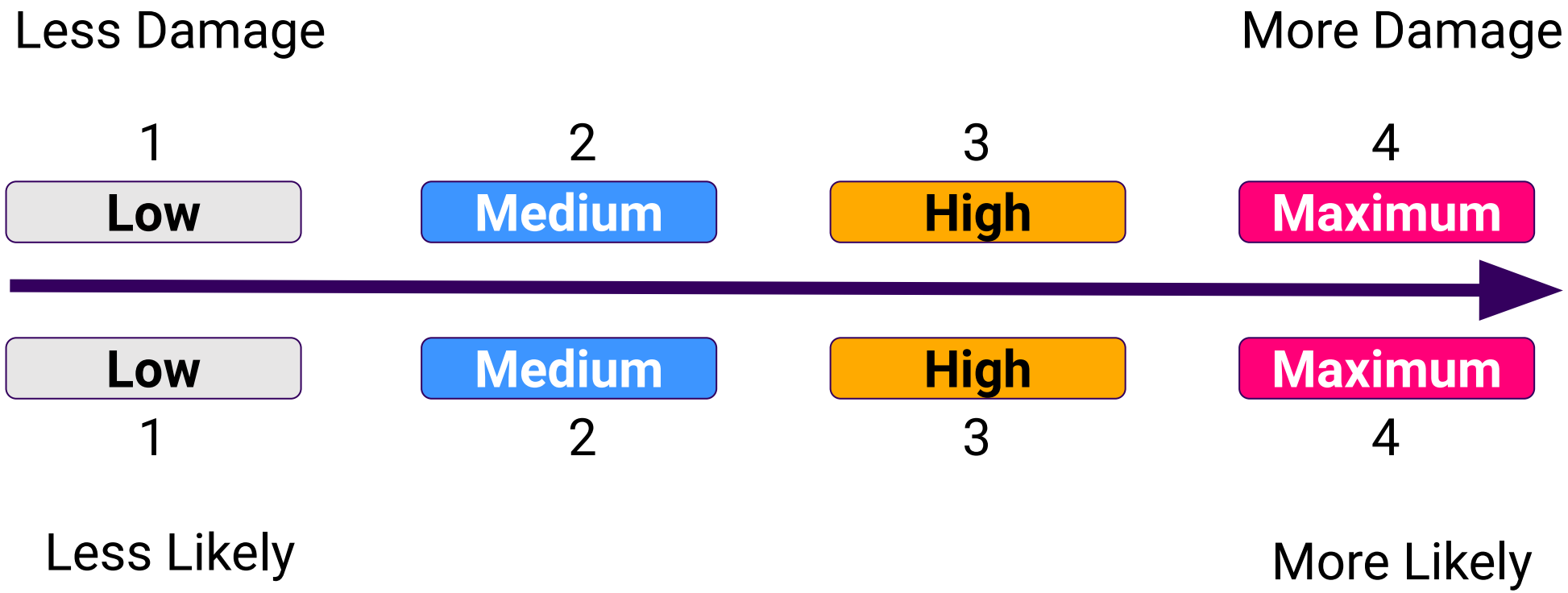
Headline news?
Brand damage
Customer trust

How long to restore?
How much forensics?
Time to rollback?
Employee Safety
Doxxing

Fines!
Legal damages
Identity insurance

DATADOG

Risk in the age of tech



Risk in the age of tech

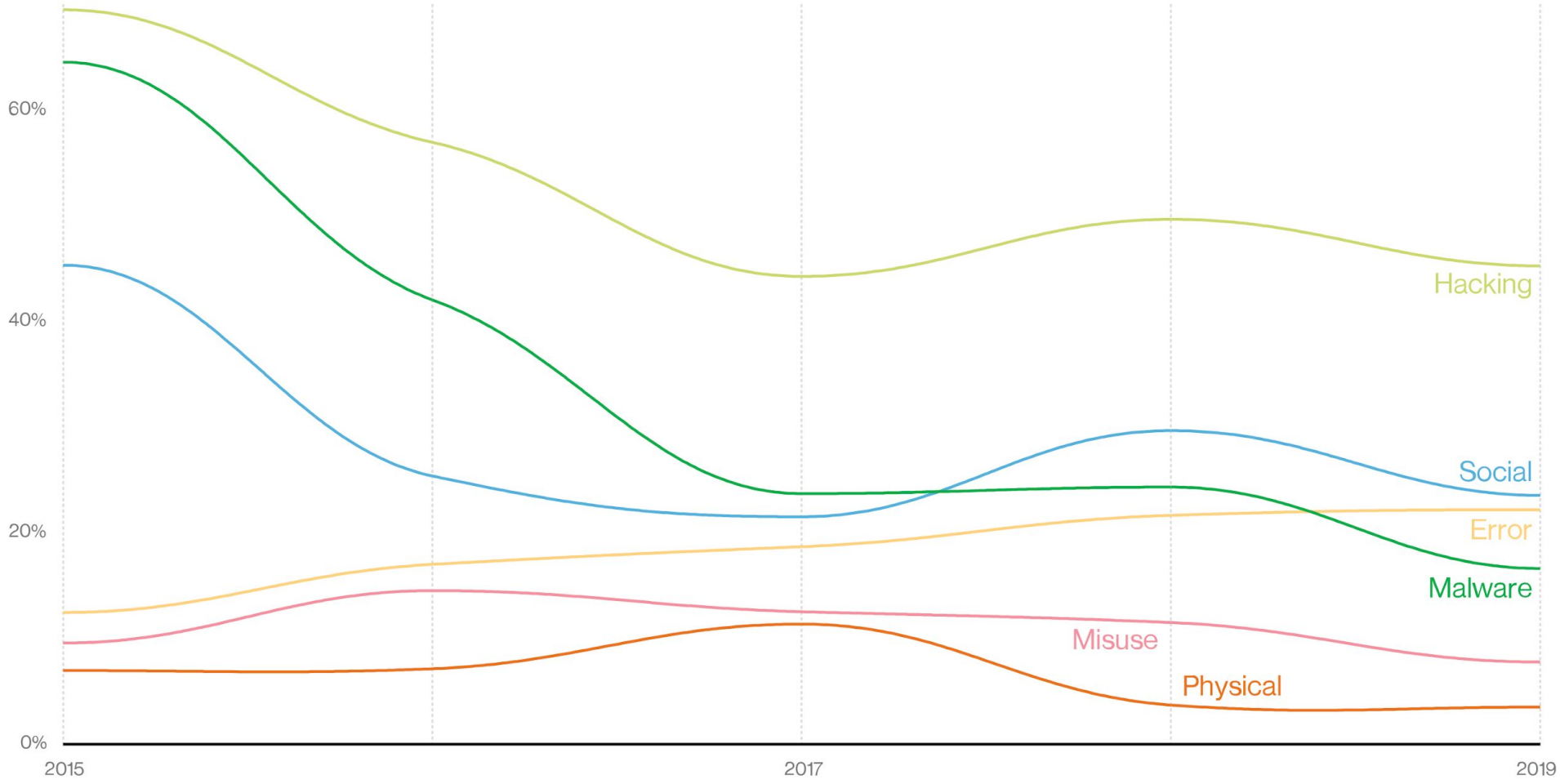


Figure 11. Actions over time in breaches

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

Risk in the age of tech

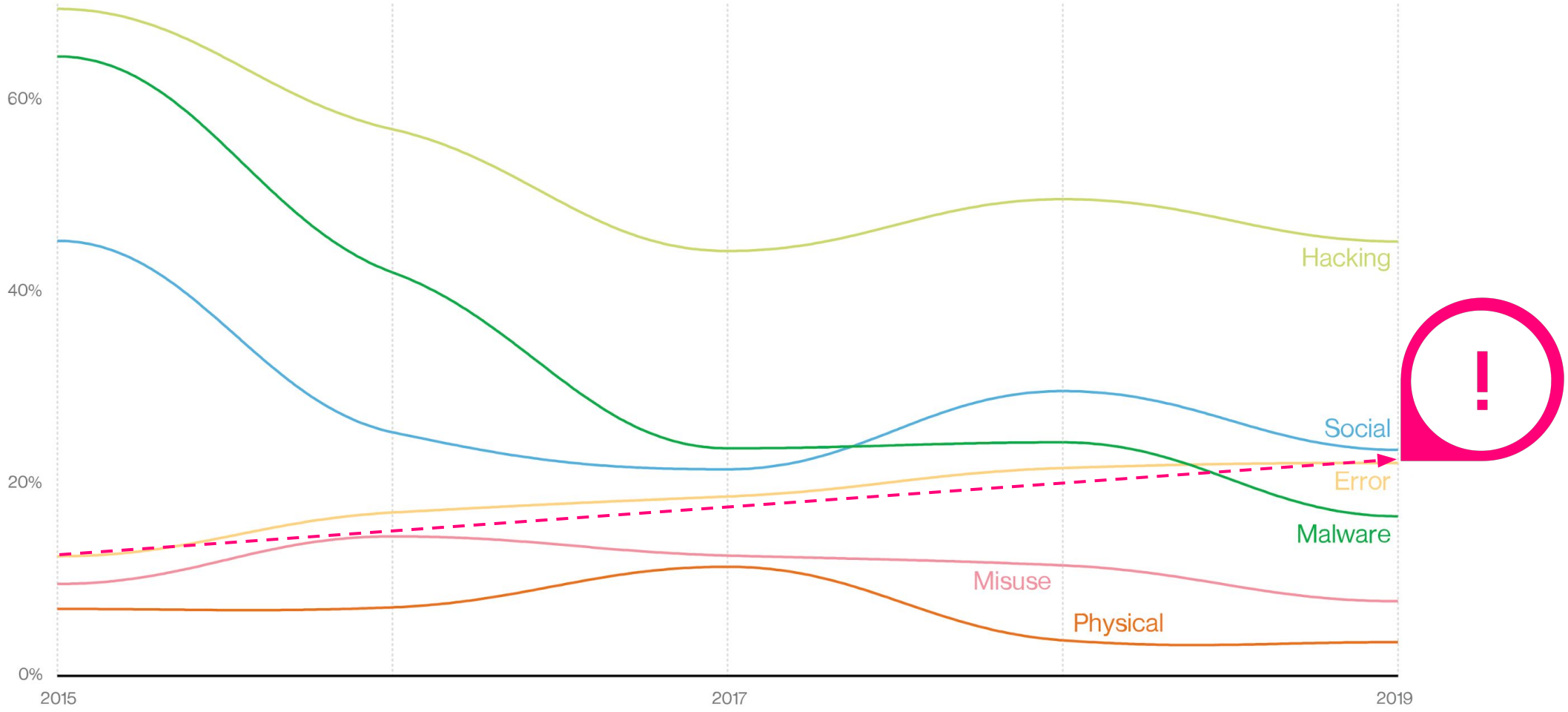


Figure 11. Actions over time in breaches

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

DATADOG

Risk in the age of tech

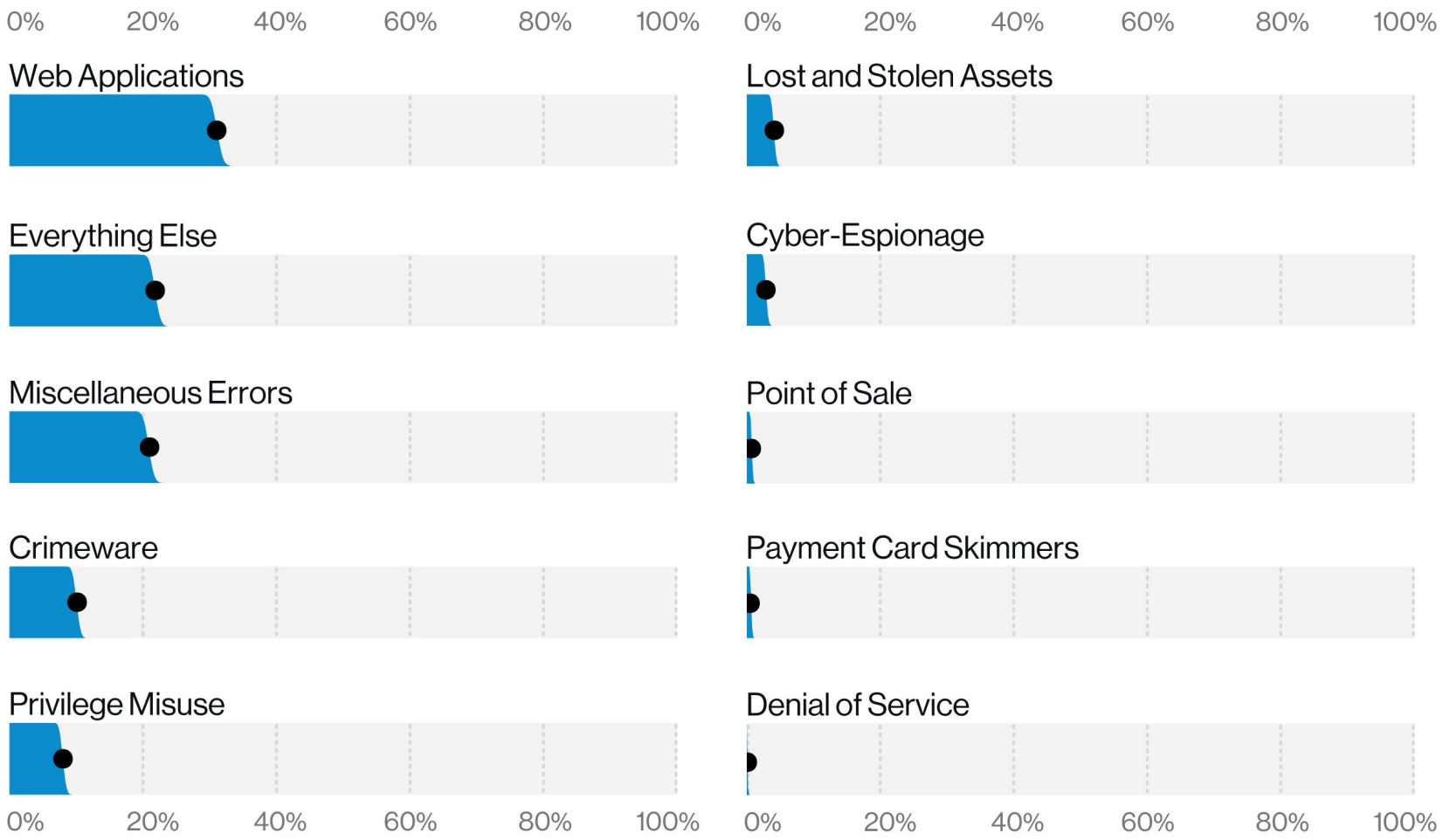


Figure 46. Patterns in breaches (n = 3,950)

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

Risk in the age of tech, *in tech itself*

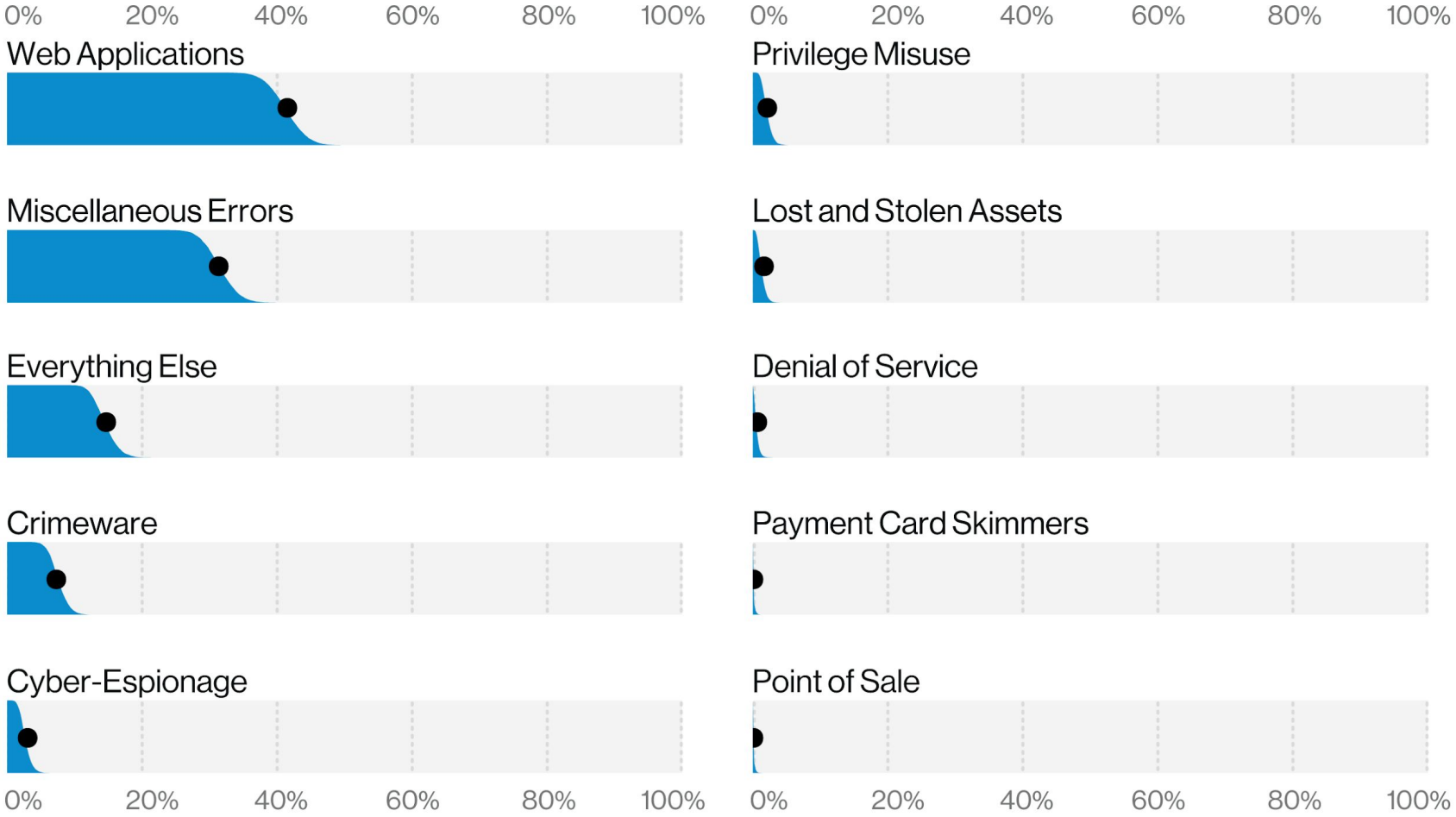


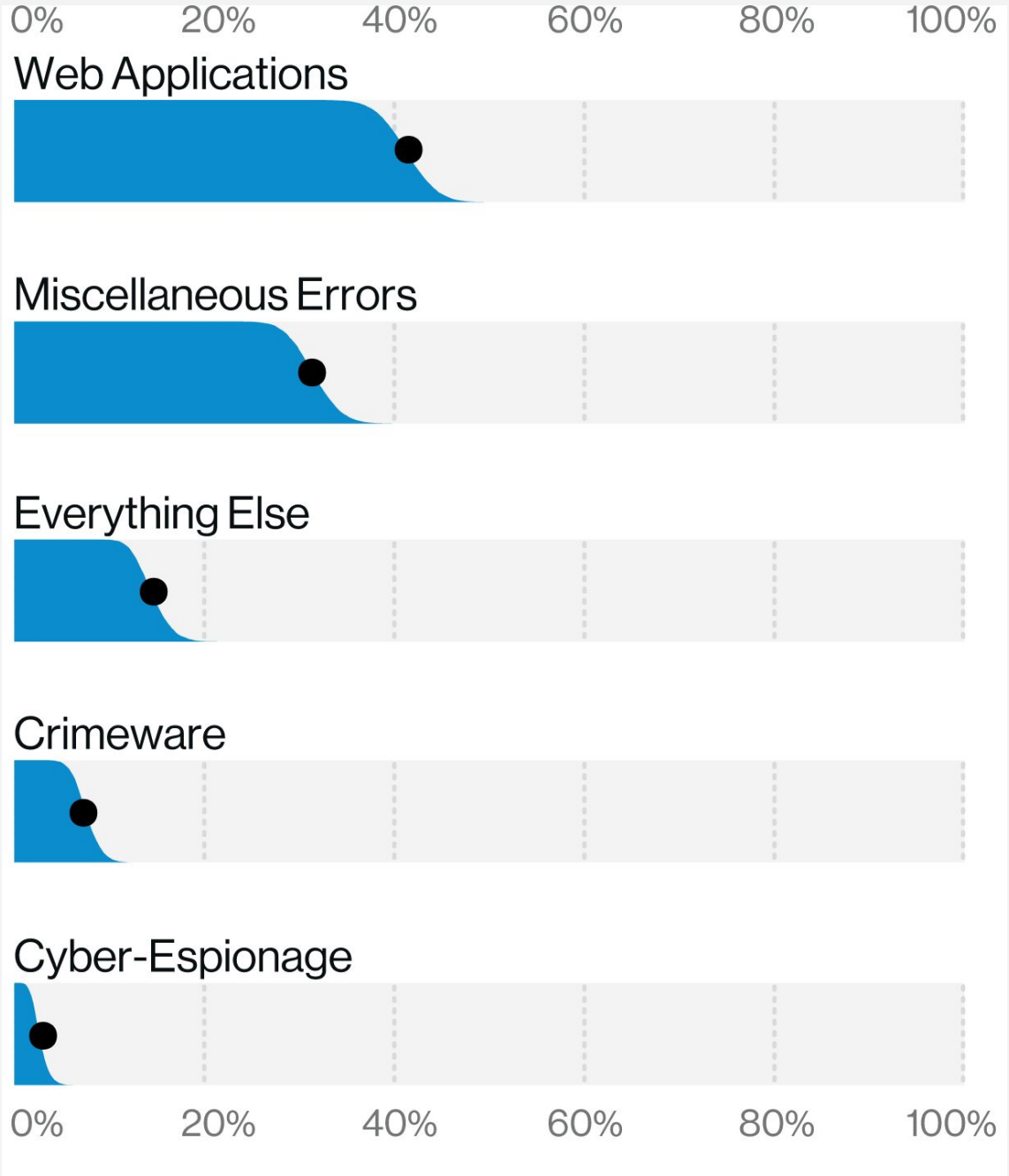
Figure 72. Patterns in Information industry breaches (n = 360)

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

Shifting-left in order to deal with specific risk

Where can we shift left?
Or get some tooling maybe?

- Web Applications
  - *Mostly vulnerabilities*
- Miscellaneous Errors
  - *Mostly misconfigs and misfires*
- Everything Else
  - *Mostly phishing*



G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

DATADOG

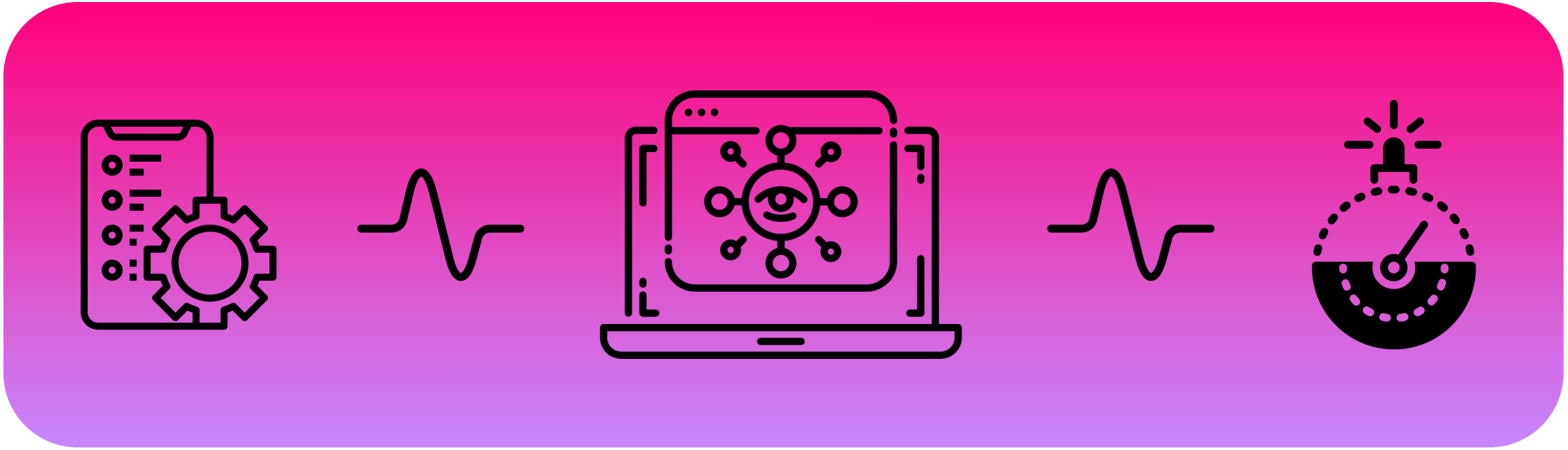
Where can we shift left?
Or get some tooling maybe?

- Web Applications
  - *Mostly vulnerabilities*
- Miscellaneous Errors
  - *Mostly misconfigs and misfires*
- Everything Else
  - *Mostly phishing*

G. Basset, S. Widup, P. Langlois, A. Pinto, and C. D. Hylender, "2020 Data Breach Investigations Report," *Verizon DBIR*, 2020. [Online]. Available: https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/. [Accessed: 15-Oct-2020].

DATADOG

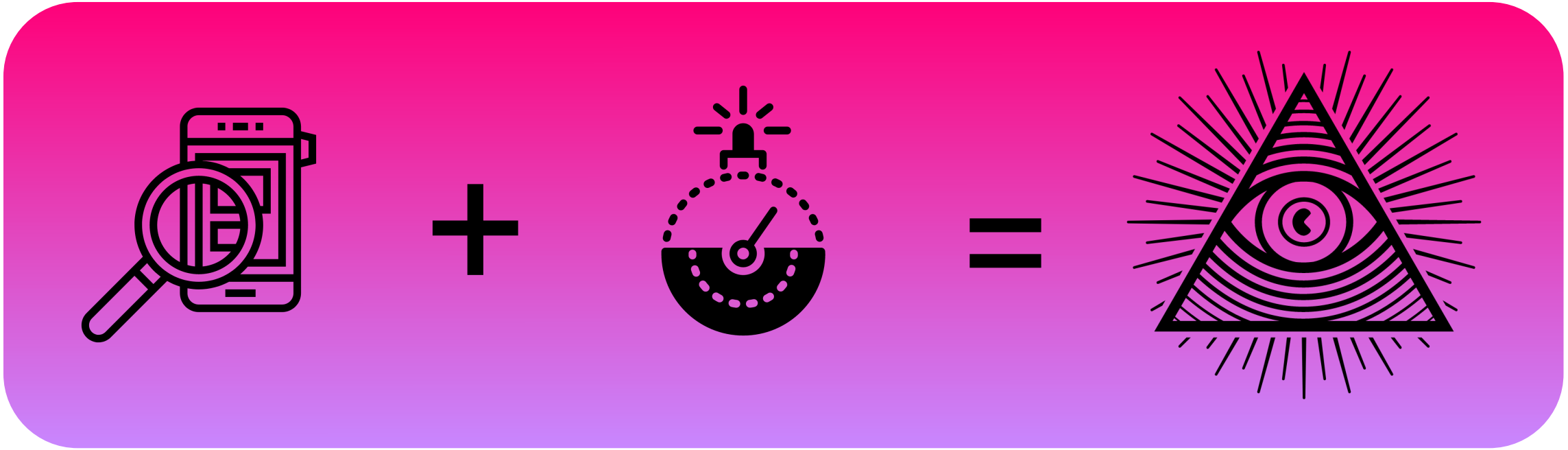
Shifting-left with regards to risk
Risk budgets for some?



Tools | Signal | Visibility & Detection | Signal | Time-based risk

DATADOG

Shifting-left with regards to risk
Risk budgets for most?



Qualitative risk

Time-based risk

Comprehensive Visibility

https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html

Shifting left with regards to risk
What is your risk budget based on?

Shifting left with regards to risk
Base your budget on your data!

It’s demo time!

Demo time!

```
risk_record = dict(
    link="https://docs.google.com/document/d/1xNVV1491IbD7e3Mnle2ztEdJbnMKiyCEVT0zYDTt7to",
    name="home.andrewkrug.com",
    service_owner="Andrew Krug",
    director="Donna Noble",
    recommendation_count=1,
    service_data_classification="staff_confidential",
    highest_risk_impact="high",
    highest_recommendation="maximum",
    creation_date=datetime.now().isoformat(),
    modification_date=datetime.now().isoformat()
)
```

event_probability = (recommendations * max_impact)

a.k.a the more things are wrong the more likely an incident will occur

MOZILLA CONFIDENTIAL - STAFF AND NDA'D MOZILLIANS ONLY

RRA for home.andrewkrug.com

Service Owner(s)	Andrew Krug
Owner's Director	Donna Noble
Service Data Classification	**Staff Confidential**
Highest Risk Impact	**HIGH**

Service Notes

How does the service work? Do we have diagrams, demos, examples? Is the service in production yet? Can we break this service down per components?

RRA Request bug:
Vendor questionnaire (if vendor):

Data Dictionary

Data name / type	Classification	Comments
DNS Logs	**Individual Confidential**	

DATADOG

Demo time!

```
risk_record = dict(
    link="https://docs.google.com/document/d/1xNVV1491IbD7e3Mnle2ztEdJbnMKiyCEVT0zYDTt7to",
    name="home.andrewkrug.com",
    service_owner="Andrew Krug",
    director="Donna Noble",
    recommendation_count=1,
    service_data_classification="staff_confidential",
    highest_risk_impact="high",
    highest_recommendation="maximum",
    creation_date=datetime.now().isoformat(),
    modification_date=datetime.now().isoformat()
)
```

DATADOG

INFO **Oct 15, 2020 at 08:31:38.746** (21 hours ago) View in Context Export

SERVICE
home.andrewkrug.com

SOURCE
risk_record

ALL TAGS
environment:production source:risk_record

Event Attributes Metrics


```
{
  creation_date            2020-10-15T03:23:59.853939
  data_score               2
  director                 Donna Noble
  event_id                 544260386b09478390d9bc664eab830a
  highest_recommendation   maximum
  highest_risk_impact      high
  impact_score             4
  link                     https://docs.google.com/document
                           /d/1xNVV1491IbD7e3Mnle2ztEdJbnMKiyCEVT0zYDTt7to
  modification_date        2020-10-15T03:23:59.853959
  name                     home.andrewkrug.com
  probability              5
  recommendation_count     1
  service                  home.andrewkrug.com
  service_data_classification  staff_confidential
  service_owner            Andrew Krug
  status                   INFO
}
```


Use ↑ / ↓ to view previous/next log

DATADOG

Demo time!

INFO **Oct 15, 2020 at 08:31:38.746** (21 hours ago)

View in Context | Export

SERVICE
home.andrewkrug.com

SOURCE
risk_record

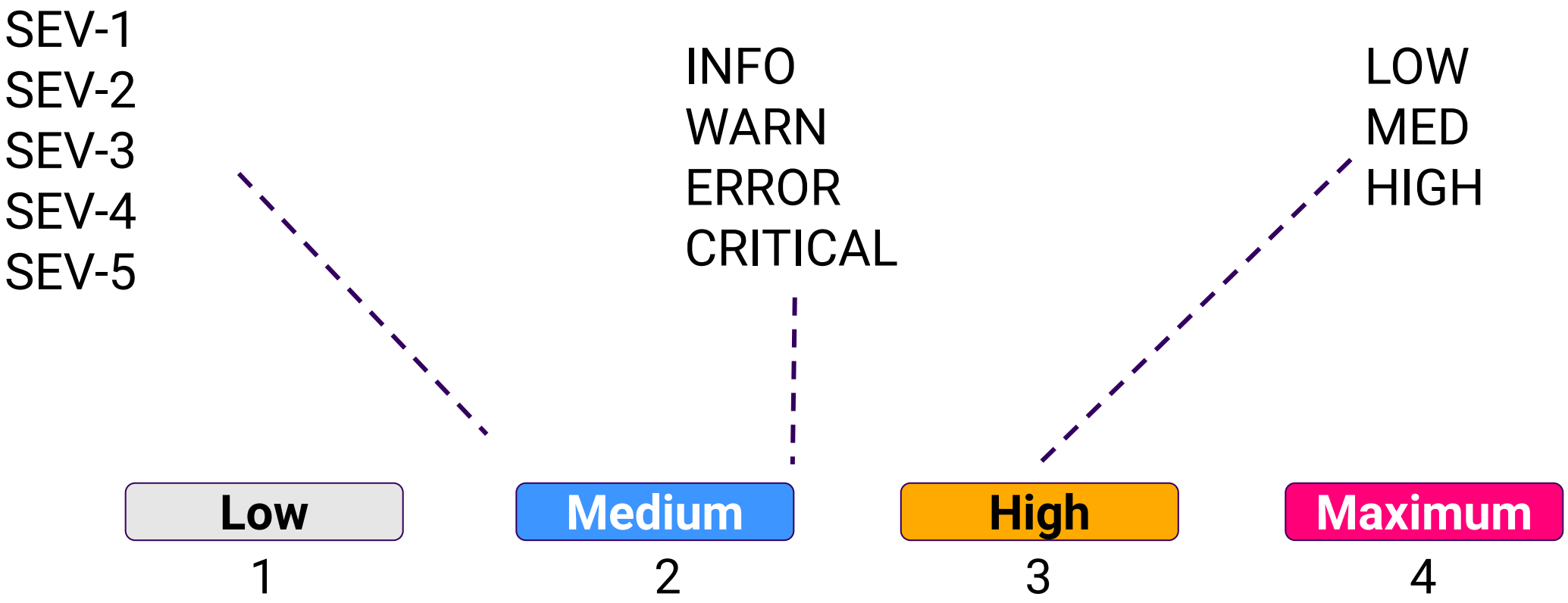
ALL TAGS
environment:production source:risk_record

Event Attributes | Metrics

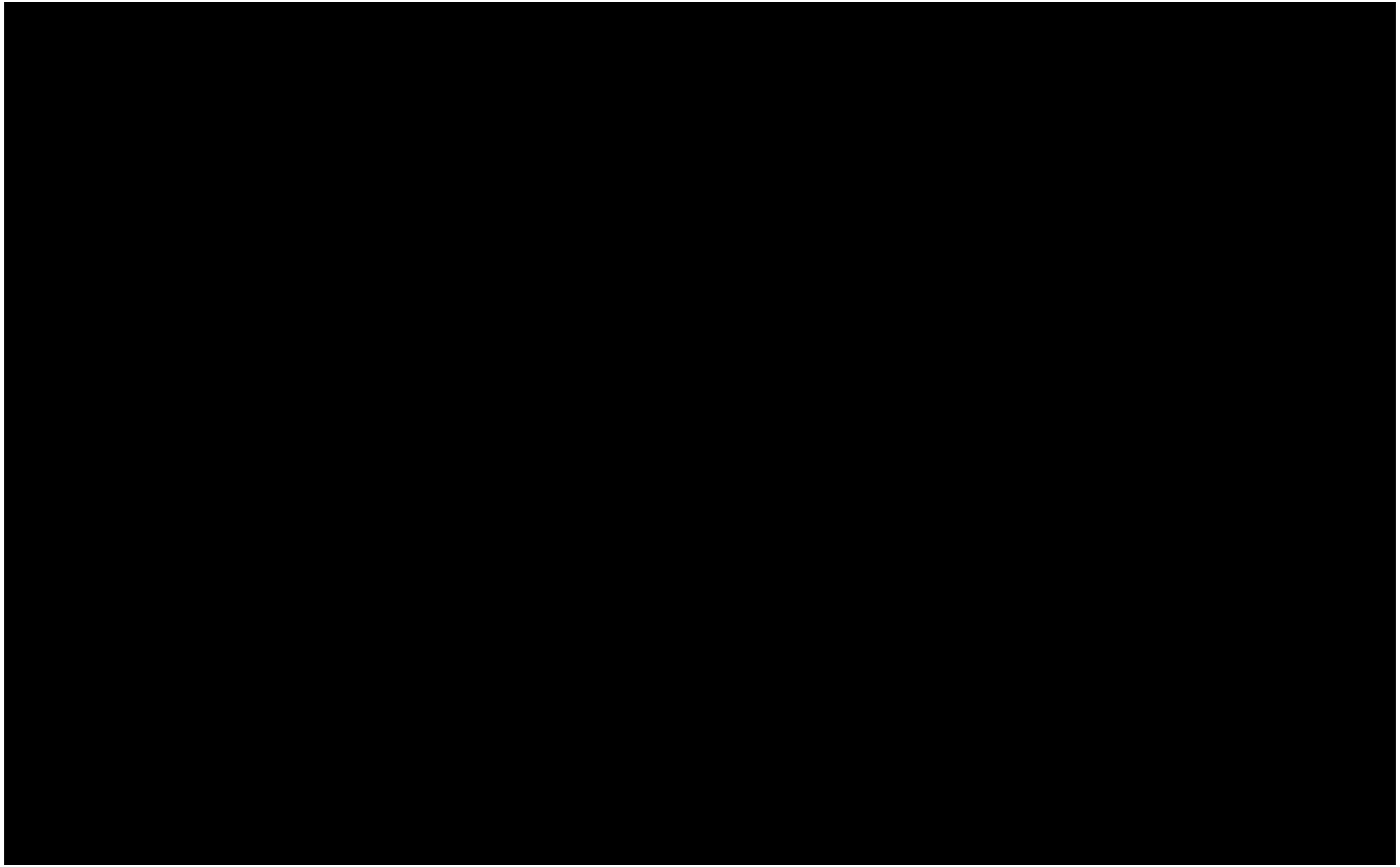

```
{
  creation_date          2020-10-15T03:23:59.853939
  data_score             2
  director               Donna Noble
  event_id               544260386b09478390d9bc664eab830a
  highest_recommendation maximum
  highest_risk_impact    high
  impact_score           4
  link                   https://docs.google.com/document
                         /d/1xNVV1491IbD7e3Mnle2ztEdJbnMKiyCEVT0zYDTt7to
  modification_date      2020-10-15T03:23:59.853959
  name                   home.andrewkrug.com
  probability            5
  recommendation_count   1
```


DATADOG

Show some tools that add risk



Example : CFN_Nag



DATADOG

Dynamic Risk

A method for calculating : Assign a weight to the number of findings

Low	Medium	High	Maximum
1	2	3	4

WARNING = 1 point
CRITICAL = 20 points

likelihood = (points * 0.25)
Since we're using a 4 point scale

```
"id": "W41",
"type": "WARN",
"message": "S3 Bucket should have encryption option set",
```

Ship that to an aggregator

Log Explorer | Save As

source:dynamic_risk_record

Facets | Saved Views | Hide Controls | 2 results four

Search facets

Showing 64 of 65 | Add

CORE

Source
- cloudtrail -
- s3 -
- dynamic_risk_record 2

Host

Service
- parker.biz 2

Status
- Error 0
- Warn 0
- Info 2

WEB ACCESS

LAMBDA

VPC

HOST	SERVICE	CONTENT
	parker.biz	{"likelih
	parker.biz	{"reason"

INFO Oct 16, 2020 at 05:12:26.043 (37 minutes ago)

View in Context | Export

SERVICE: parker.biz

SOURCE: dynamic_risk_record

ALL TAGS: environment:production source:dynamic_risk_record

Event Attributes | Metrics


```
{
  creation_date    2020-10-16T12:09:17.284384
  event_id         21c15dc2b48e4677bee5fc59f48e0668
  likelihood_score 4
  name             parker.biz
  reason [
    {"filename":"bucket_with_no_policy.yml","file_results":
    {"violations":[{"logical_resource_ids":["Bucket2"],"line_numbers":
    [15],"id":"W51","type":"WARN","message":"S3 bucket should likely
    have a bucket policy"},{"logical_resource_ids":
    ["Bucket","Bucket2"],"line_numbers":
    [3,15],"id":"W35","type":"WARN","message":"S3 Bucket should have
    access logging configured"},{"logical_resource_ids":
    ["Bucket","Bucket2"],"line_numbers":
    [3,15],"id":"W41","type":"WARN","message":"S3 Bucket should have
    encryption option set"}],"failure_count":0}}
  ]
  service          parker.biz
  status           INFO
}
```


Use ↑ / ↓ to view previous/next log

DATADOG

$$R = f(s, p, c, k)$$

Risk Screenboard

Edit Widgets

4h Past 4 Hours

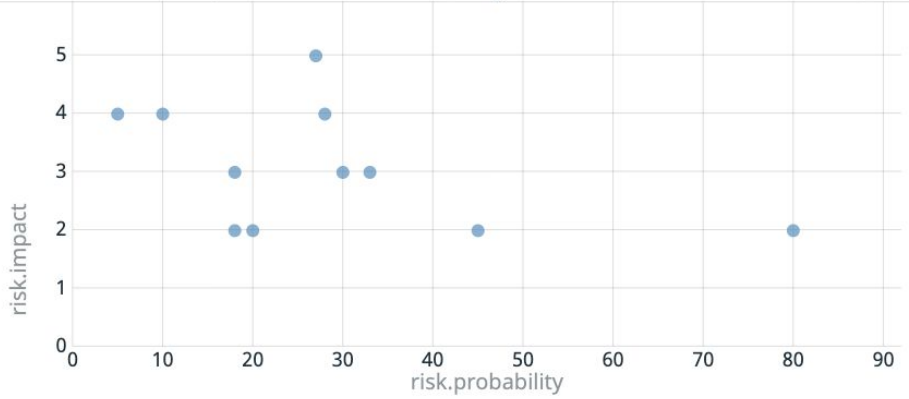
Add Template Variables

Avg of risk.impact over *

3

Global Risk Impact and Probability Over Time

2d



Inbound Dynamic Risks

↓ DATE	HOST	SERVICE
Oct 16 05:12:26.043		parker.biz

{"likelihood_score":4,"reason":
[{"filename":"bucket_with_no_policy.yml","file_resu
lts":{"violations":[{"logical_resource_ids":

Oct 16 05:09:32.368		parker.biz

{"reason":
[{"filename":"bucket_with_no_policy.yml","file_resu
lts":{"violations":[{"logical_resource_ids":

Data Classification for Demo Service : STAFF_CONFIDENTIAL

DATADOG

So in summary…

In summary…
a.k.a. the tl;dr

- The best risk assessments incorporate qualitative and quantitative metrics
- Your environment is already giving you risk signals
- Risk is a tool that software development teams can add to their toolbox in order to help the business **go fast** *and* **stay safe.**
- It’s not always wrong to accept **SOME risk** depending on your risk budget.

In summary…
Keep the party going!

https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment.html

We're going to have a free risk assessment training with one of the creators (@kangsterizer) of Mozilla RRA. Email or follow us on Twitter for more info!

andrew.krug@datadog.com // **@andrewkrug**

daniel.maher@datadog.com // **@phrawzty**