Risk in Cyber Systems

Marshall Kuypers

PhD Candidate, Department of Management Science and Engineering

Stanford University

mkuypers@stanford.edu

Dr. Elisabeth Paté-Cornell

Professor, Department of Management Science and Engineering

Stanford University

mep@stanford.edu

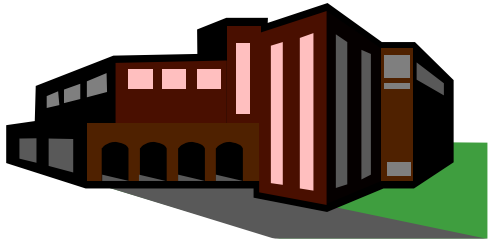
Notes meant for voice track are in blue bubbles

Presented at the Society of Risk Analysis Annual Meeting
Arlington, Virginia. December 7-9, 2015.

Our research is motivated by the idea that…

significant **uncertainty** surrounds **cyber security investments**

An organization considering three investments currently does not have a rigorous way to assess the value of different safeguards, or to quantify cyber risk.



Open DLP

Data loss prevention

Two-factor authentication

CROWDSTRIKE

Subscription for threat intel

Current methods are limiting

Organizations use 'people sitting around a table' to make decisions, or rely on hand-wavy explanations from security vendors.

PSAT

Likelihood			
Very likely	Medium 2	High 3	Extreme 5
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2
What is the chance it will happen?	Minor	Moderate	Major

Impact

Hand Waving

The cybersecurity framework in action: an Intel use case

			ENDPOINT/ DATA PROTECTION		
IDENTIFY	POLICY	NETWORK		IDENTITY	OPs
Business Environment	3	3	3	2	3
Asset Management	3	2	2	2	1
Governance	3	2	3	2	2
Risk Assessment	2	2	2	2	2
Risk Management Strategy	4	3	2	2	2
PROTECT					
		3	2	2	3
		3	3	2	3
		2	2	2	2
		2	1	3	1

Mapping highlighted outliers and major differences

If a method exists, it is likely to be qualitative: Intel published an example, but the analysis may not have been data driven

rigorous, **quantitative** methods now **exist**

Quantitative approaches lead to more insights

Data Analysis

Significant data exists in organizations!

1

Malicious Insider

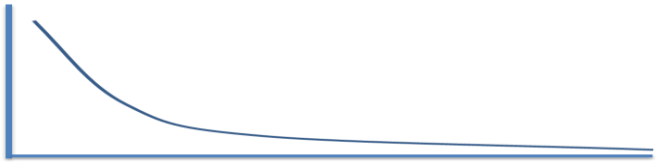
375

Website Compromises

Modeling

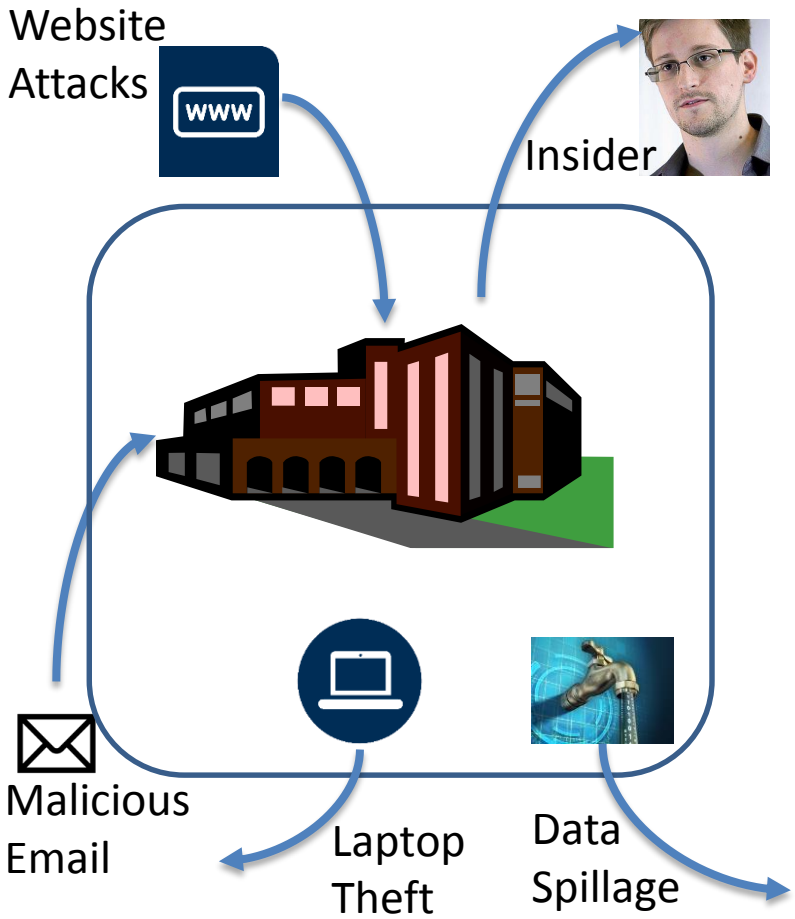
Use dollars

Use distributions, not averages



Our method is data driven, uses dollars, and uses distributions. Overall, we model the frequency and impact of different cyber attack categories and quantify risk

Risk Analysis



Our work has been successful in part because we've gotten access to security incident data. These…

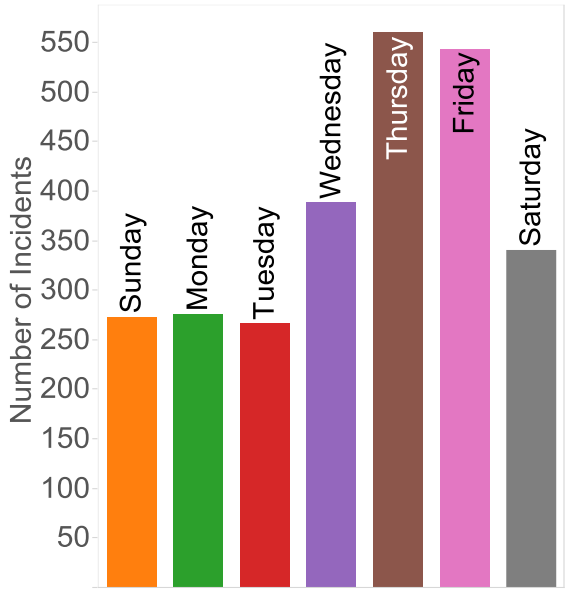
incident databases are treasure troves of **intel**

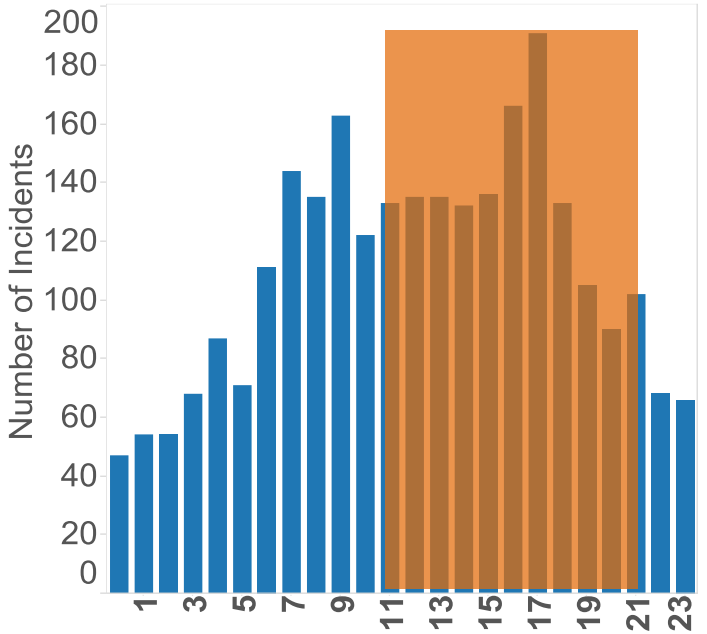
Shellshock attacks

We can analyze shellshock attacks

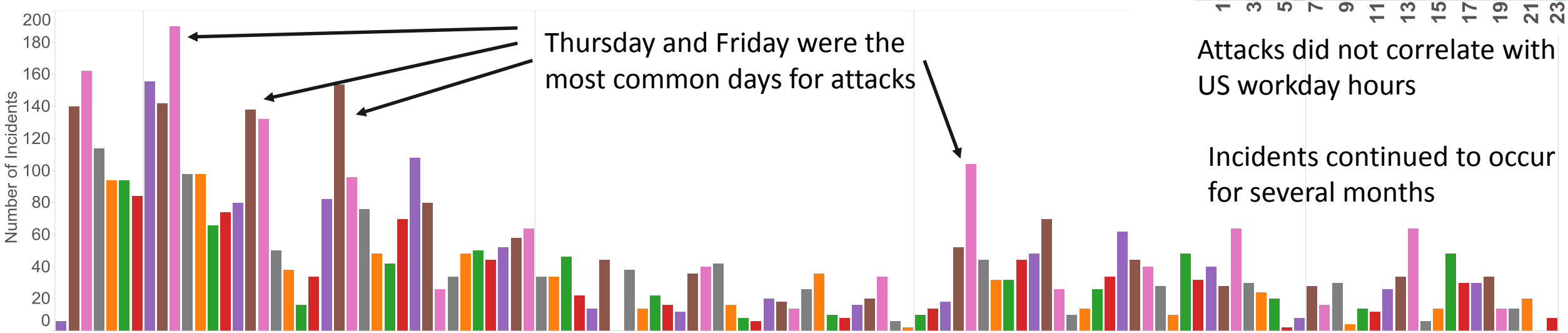
Shellshock publically announced on September 24th

Within 5 hours, a shellshock attack was detected





Attacks did not correlate with US workday hours



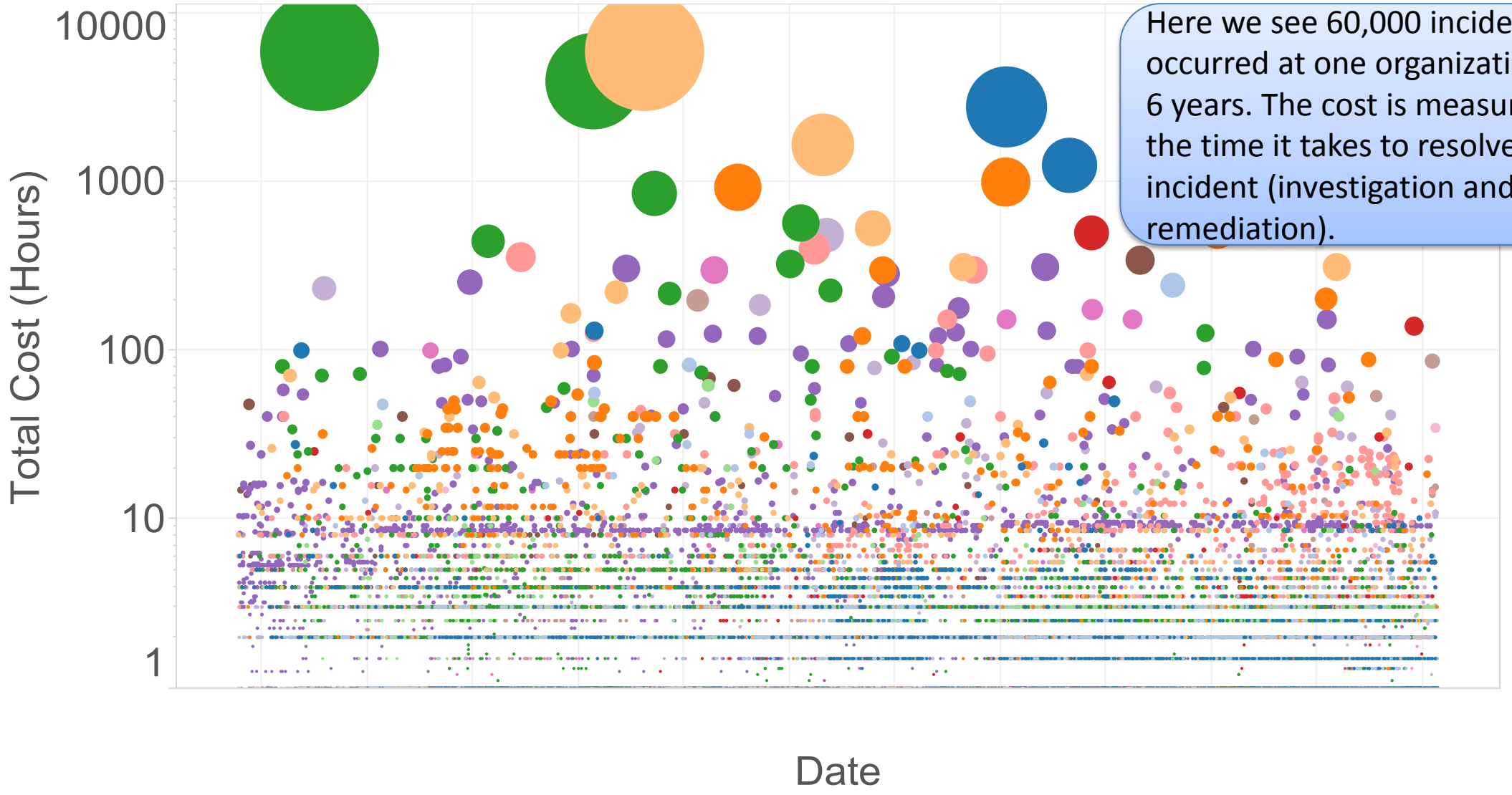
Thursday and Friday were the most common days for attacks

Incidents continued to occur for several months

We can also do a really good job of quantifying the frequency and impact of cyber security incidents.

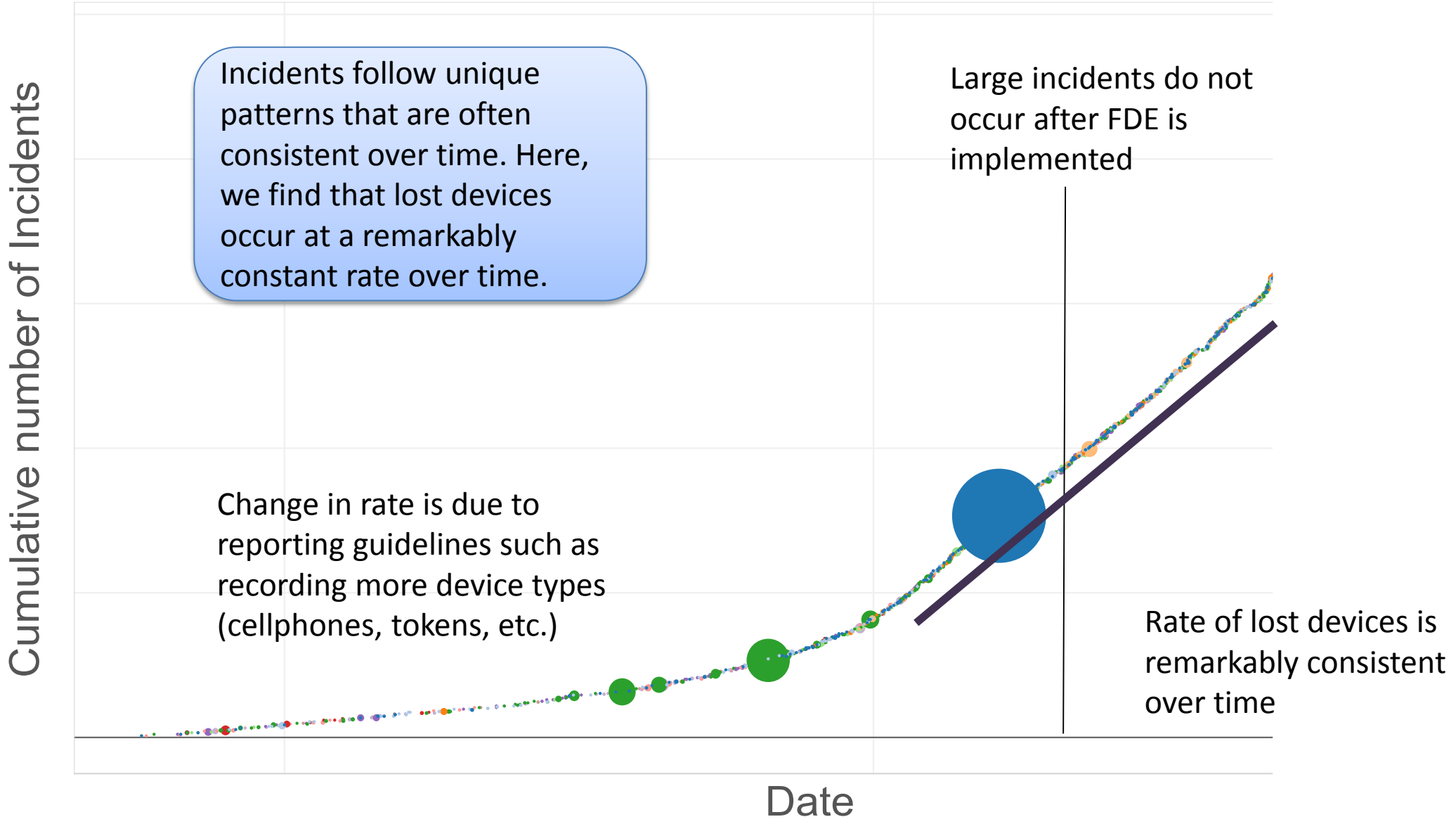
frequency and **impact** of cyber incidents can be **quantified**

Most incidents take less than 100 hours to resolve

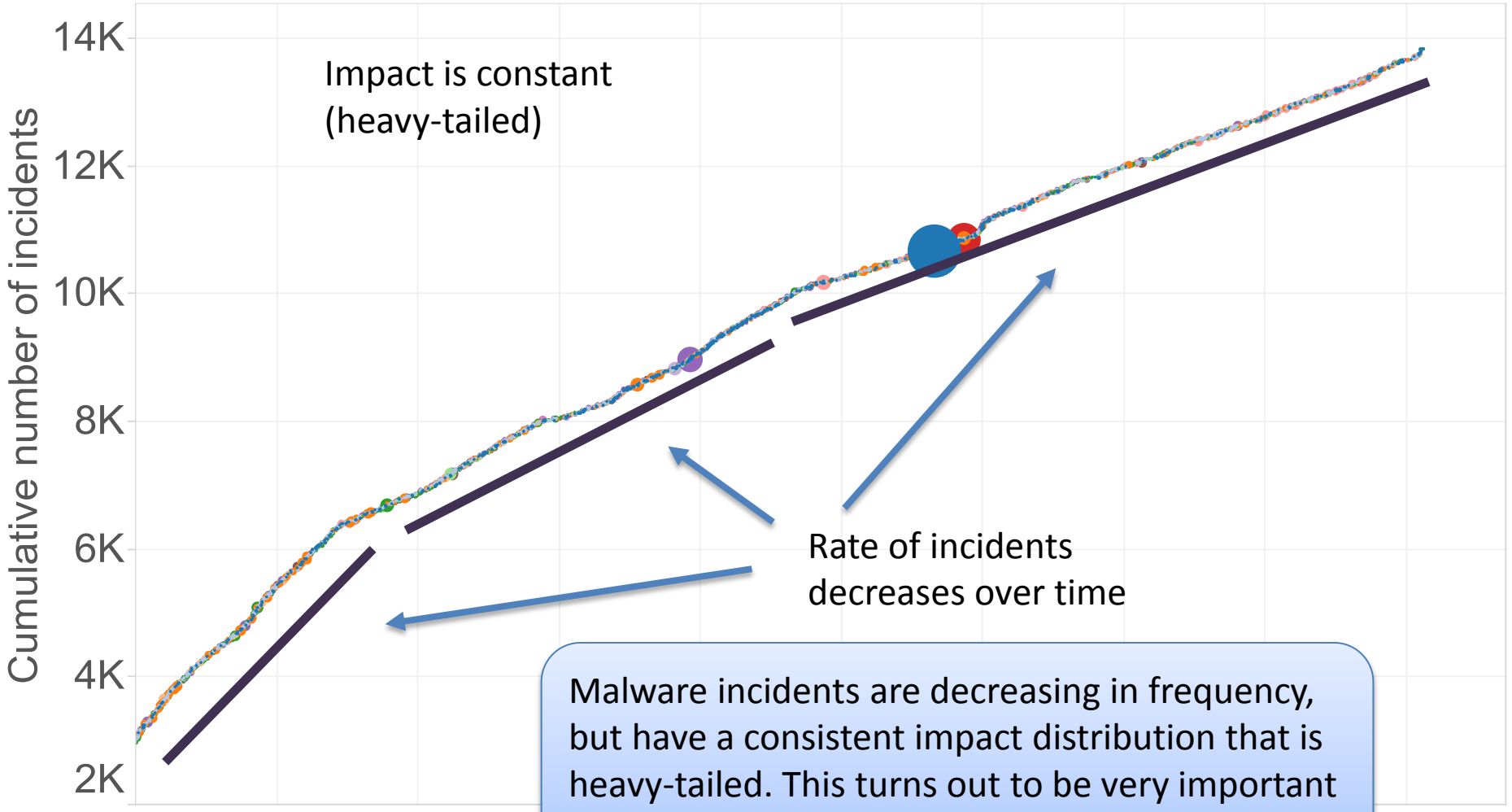


Here we see 60,000 incidents that occurred at one organization over 6 years. The cost is measured by the time it takes to resolve an incident (investigation and remediation).

Lost devices: constant rate, decreasing impact



Malware: Decreasing rate, constant impact



Malware incidents are decreasing in frequency, but have a consistent impact distribution that is heavy-tailed. This turns out to be very important for a number of reasons shown at right.

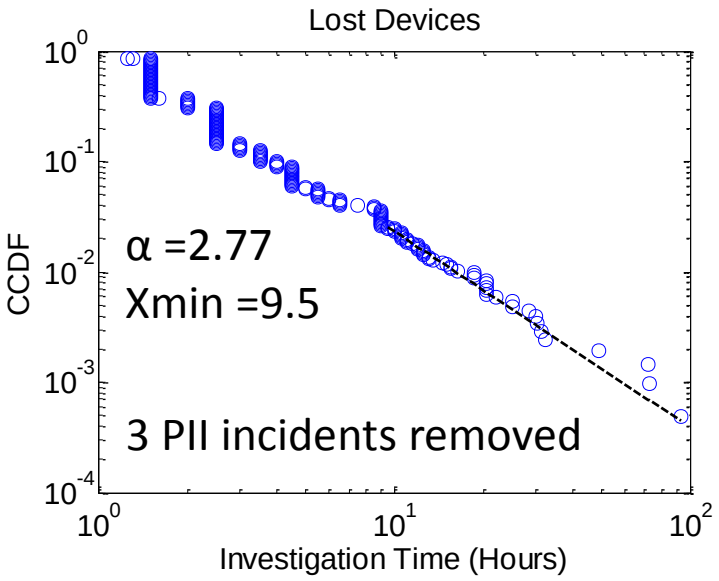
Large Events are NOT outliers

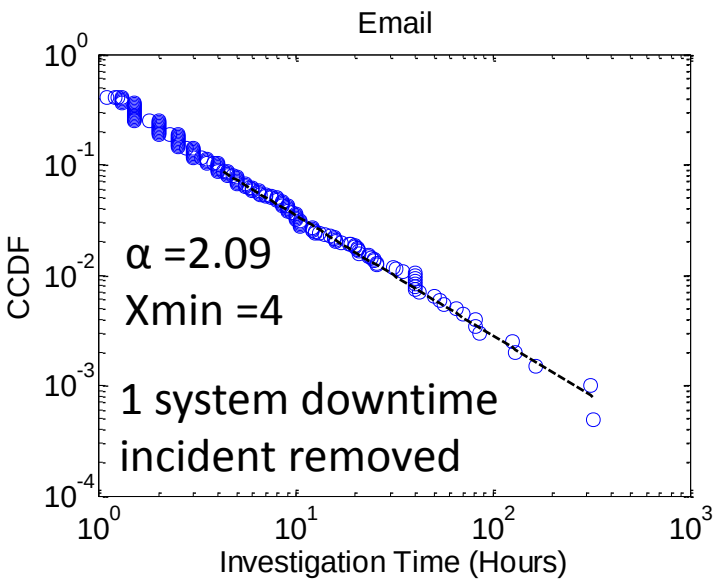
No 'average' or 'typical' cyber breach

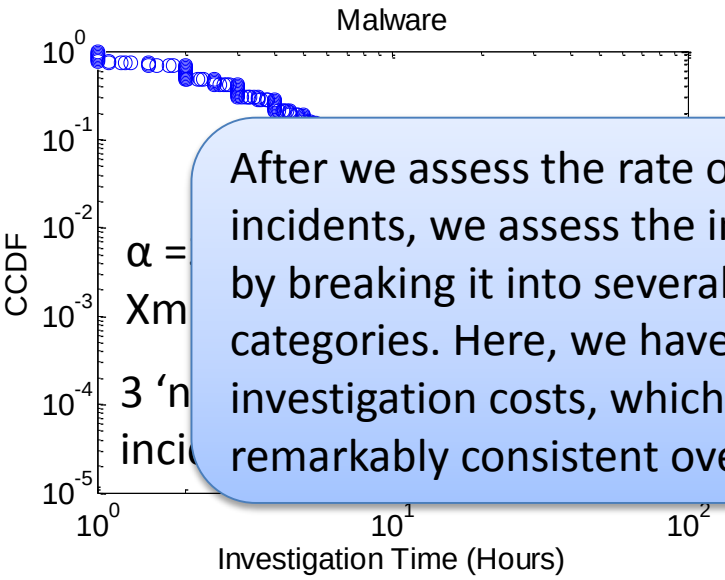
Standard deviations and some risk metrics (value at risk) are not valid

Largest incident can be more impactful than all other incidents combined!

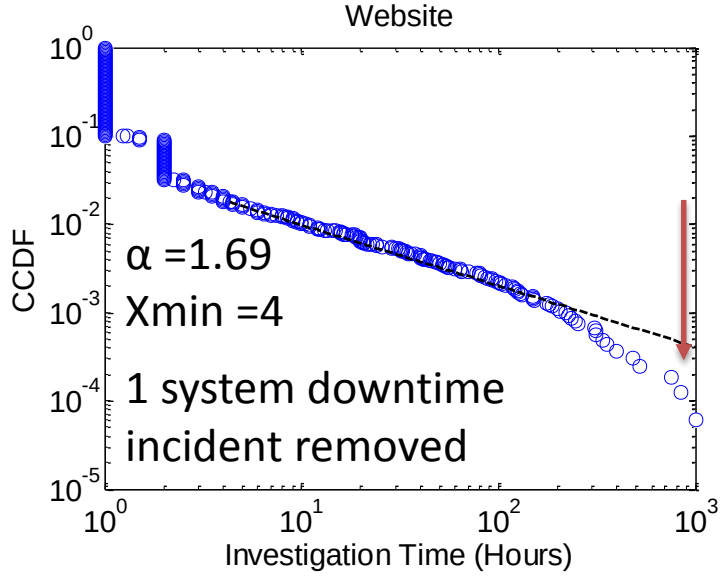
Investigation is a major cost, and can be quantified

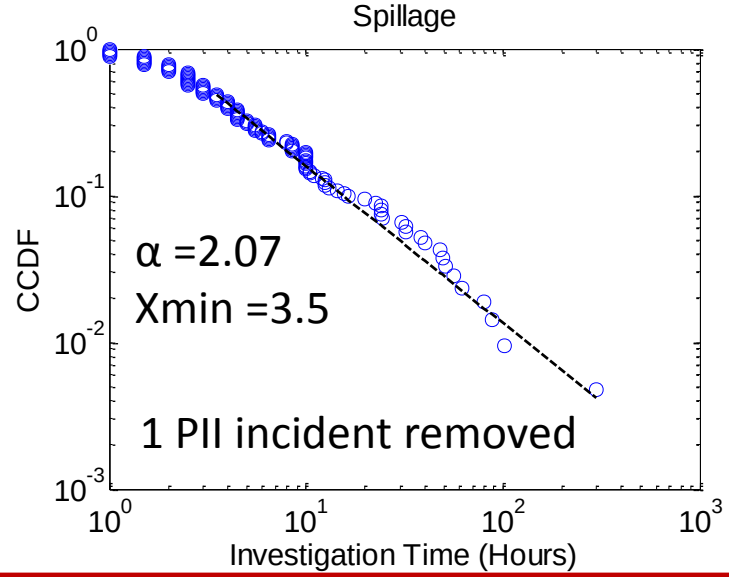


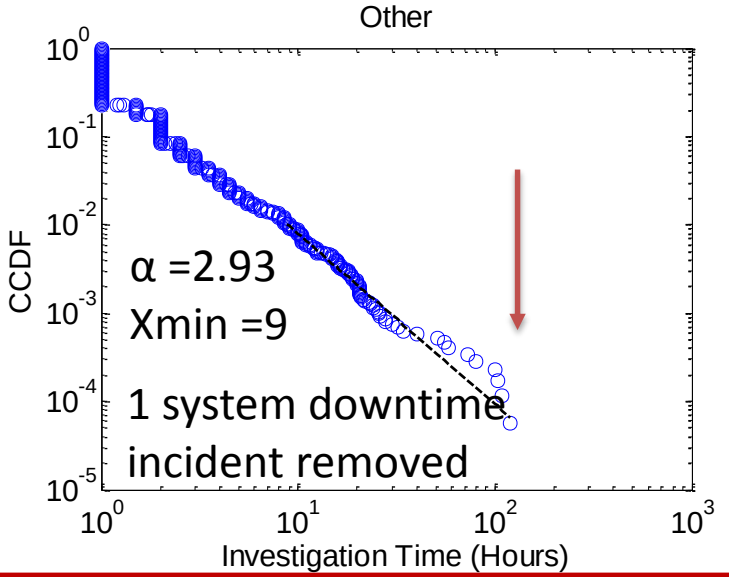




After we assess the rate of incidents, we assess the impact by breaking it into several cost categories. Here, we have data on investigation costs, which are remarkably consistent over time.

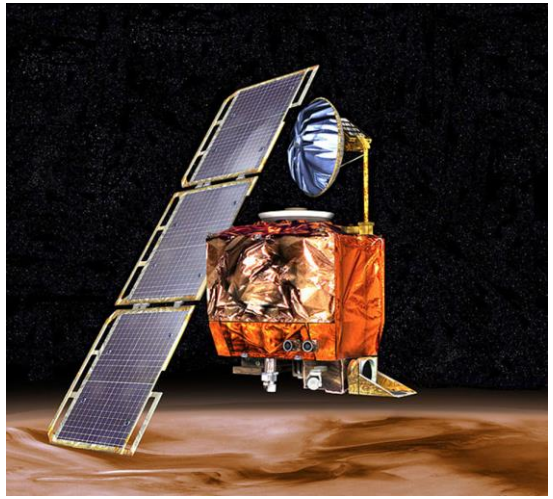






Reputation damage uncertainty is modeled

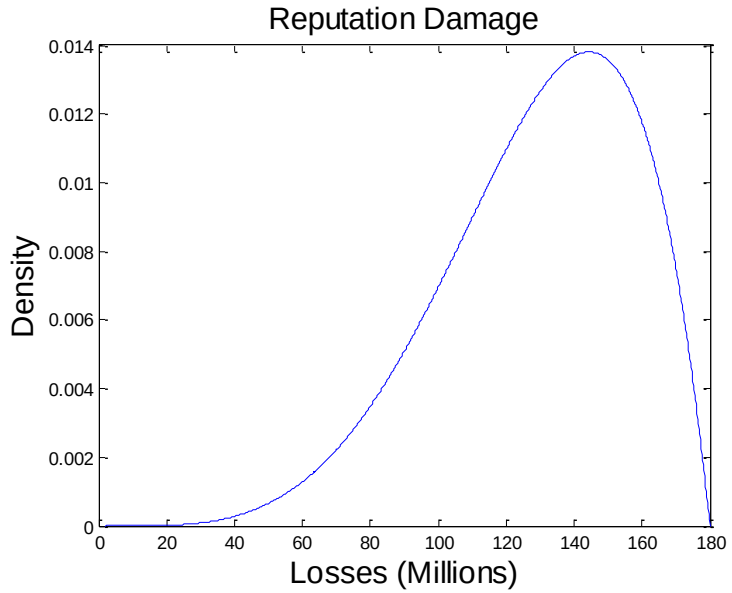
Mars Global Surveyor
Failure: 2006
Cost:$154M to build, $65 to launch, $20M per year to operate
Description: Software update error causes computer crash and fried batteries



Mars Climate Orbiter
Failure: 1999
Cost:$193M
Description: metric and standard units conversion crashes the orbiter into mars

TARGET

Reputation damage has been a hurdle in the past, but we explicitly model the uncertainty of losses (seen at right). For a case study, take chip manufacturer that stocks satellite parts. We can look at failures of satellites (that are cyber attack flavored, not attacks) to estimate costs. Academic research shows that stock prices only fall for 2 days after a breach, and we can look at Target, RSA, or Sony for other case studies.



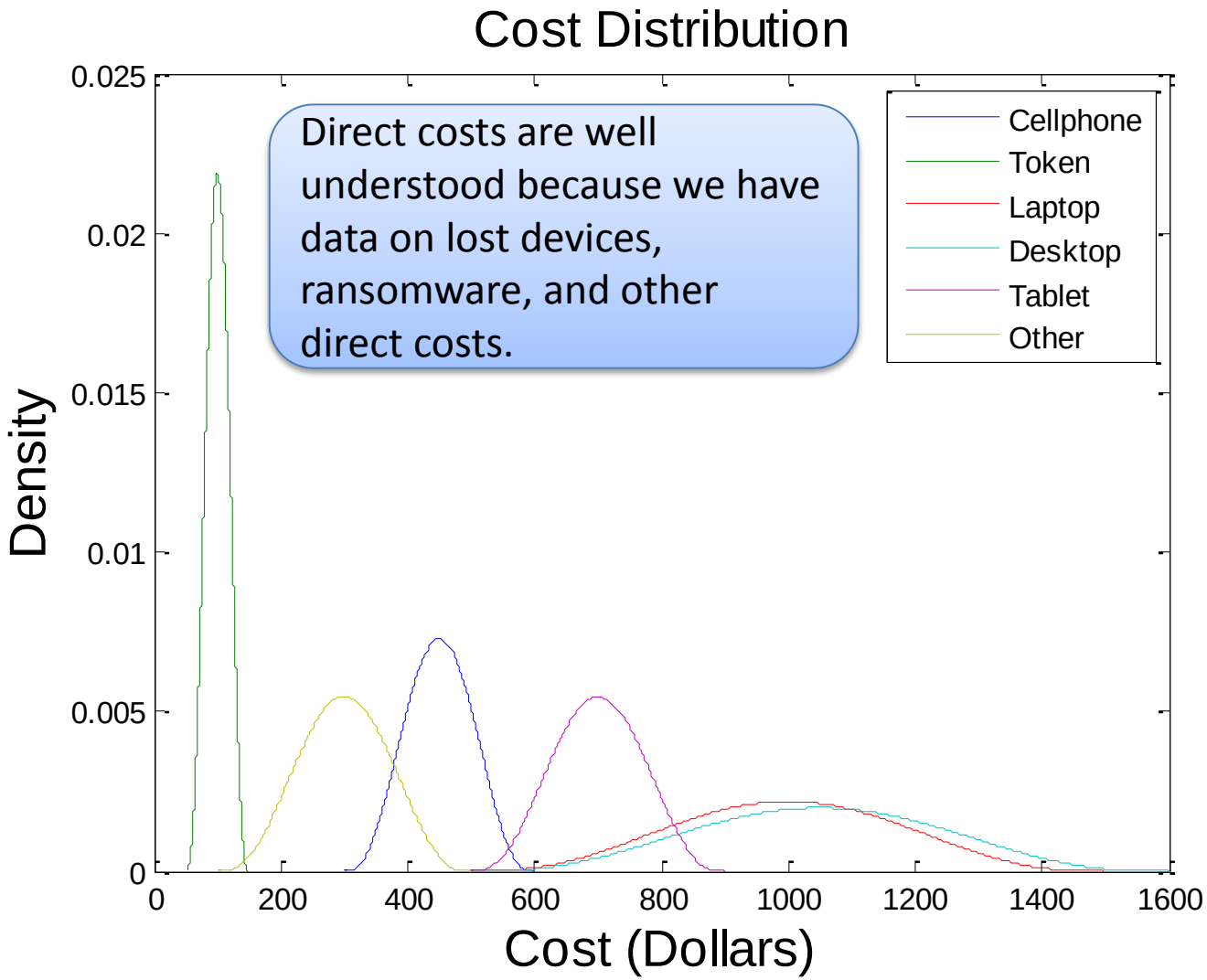
Direct costs are well understood

Probability	Device	Average Cost
0.34	Cellphone	$400
0.32	Token	$100
0.20	Laptop	$1000
0.07	Other	$300
0.05	Desktop	$1000
0.02	Tablet	$700

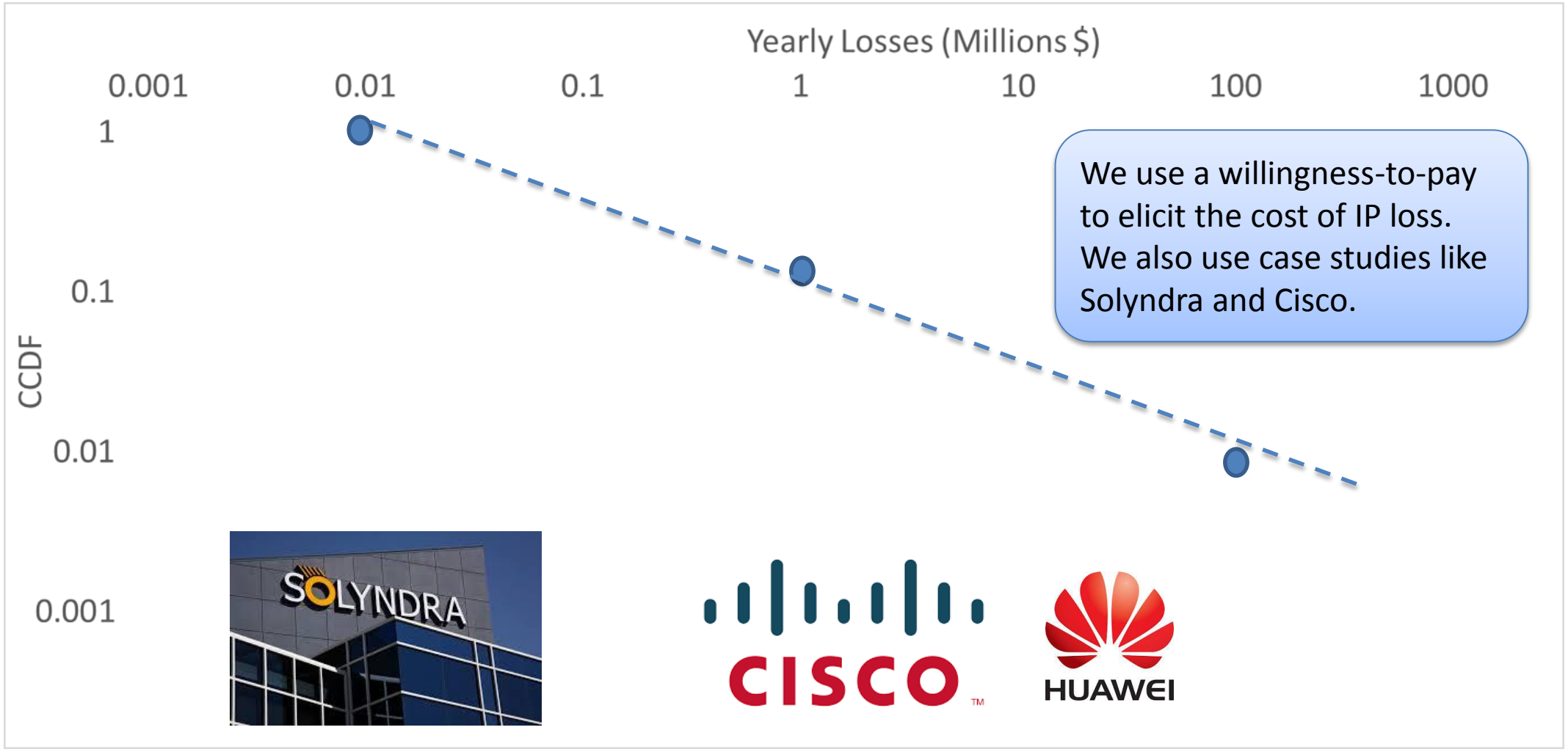
Equipment Losses

DDoS
Distributed Denial of Service Protection

Extortion



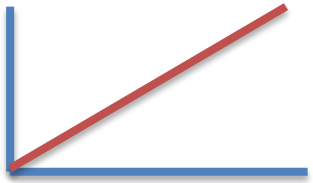
Willingness-to-pay used for intellectual property losses



rolling this **information** together, we can obtain excellent **risk assessments**

A case study demonstrates the method

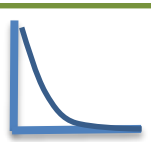
Rate of spillage incidents

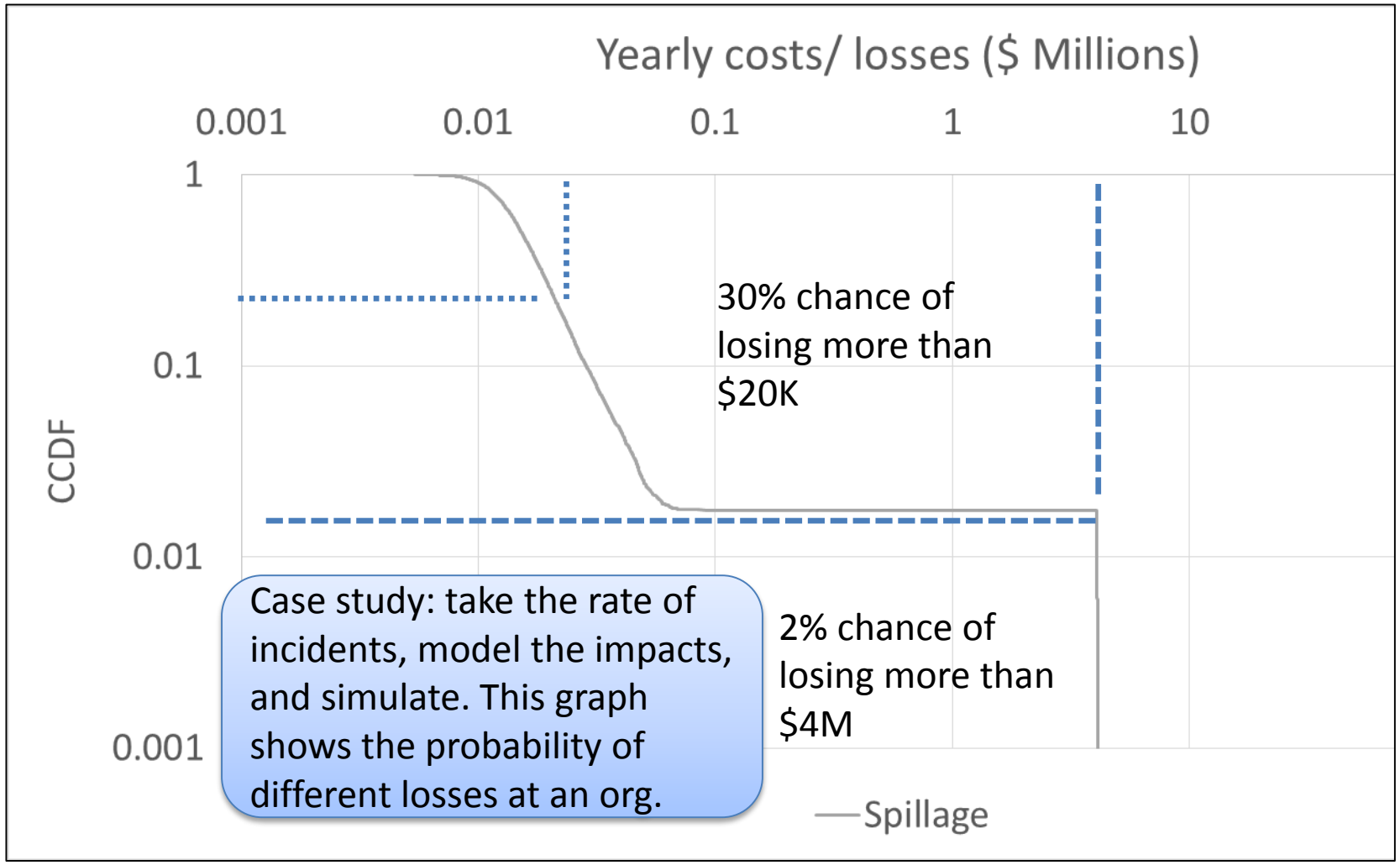


λ

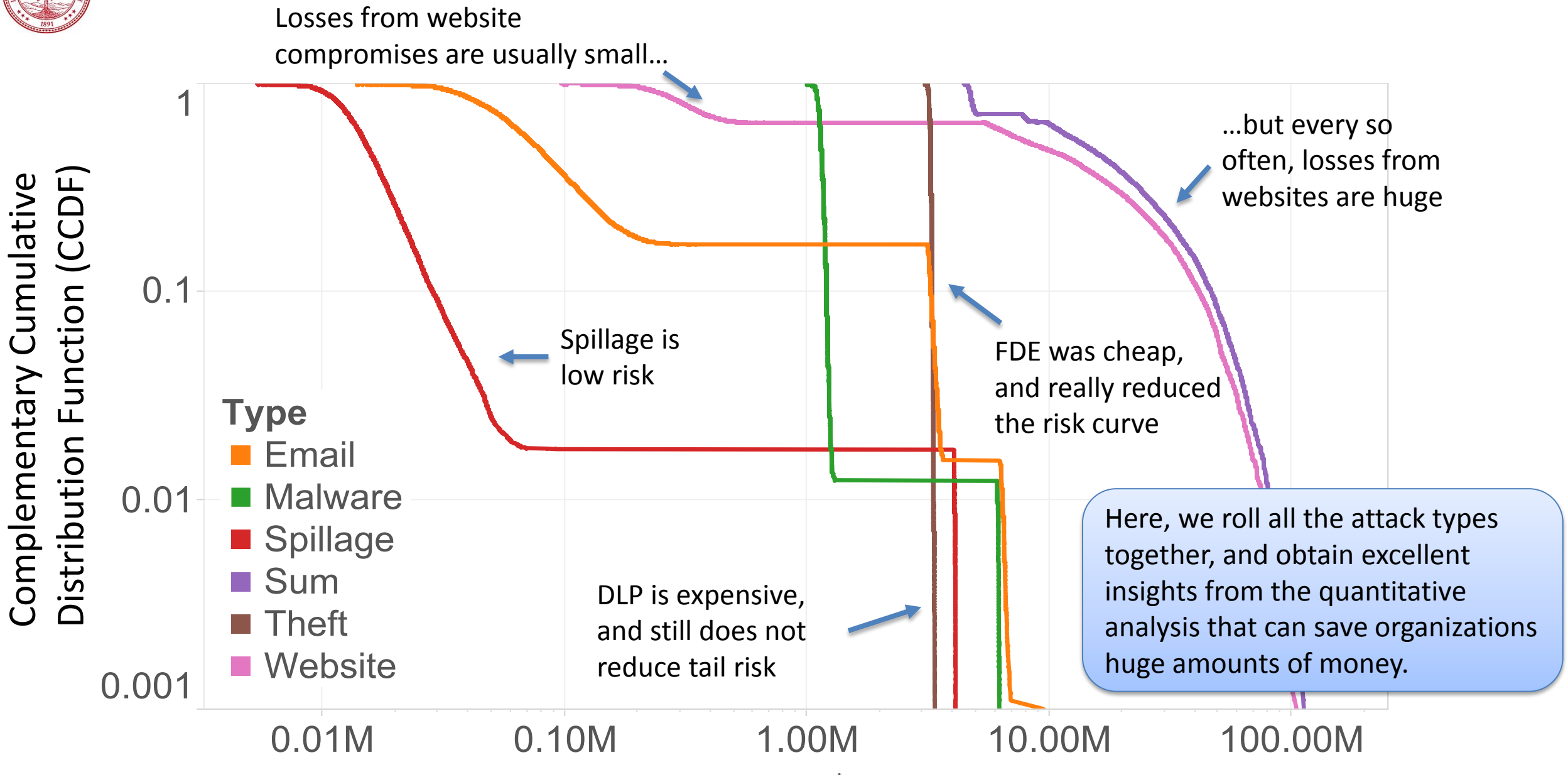
Yearly Rate: 50

Impact Distributions (Data Spillage)

Investigation	Alpha 1.22, scale 0.827
Reputation	Distribution
Fines	
IP Loss	



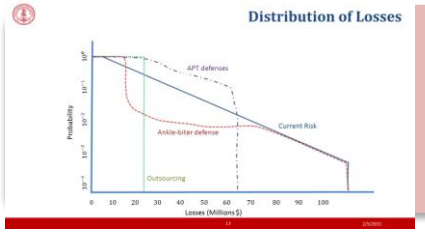
A case study demonstrates the method



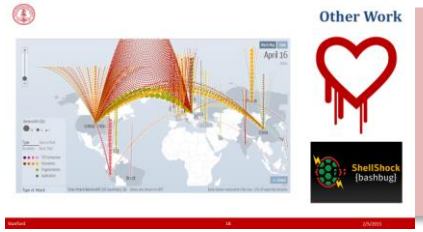
Conclusions

Probabilistic risk analysis methods inform **actionable** decisions.

Incident **data** is **priceless**.



Safeguards can be **compared** and **prioritized**.



Monetary impacts help justify **budgets** and **communicate** risk.