A hacker's adventures in Cyber Insurance

Eireann Leverett

@concinnityrisks

Your first stress test is for free...

Business Blackout

which is fine, if you like driving by looking in the rear view mirr

Types of Cyber Insurance we helped create

- Breach
- DDoS
- Financial Fraud
- Ransomware
- Cyber Physical Attacks
- Nuclear Facility Cyber Physical
- Cyber Terrorism with PoolRE

Insurers view of risk

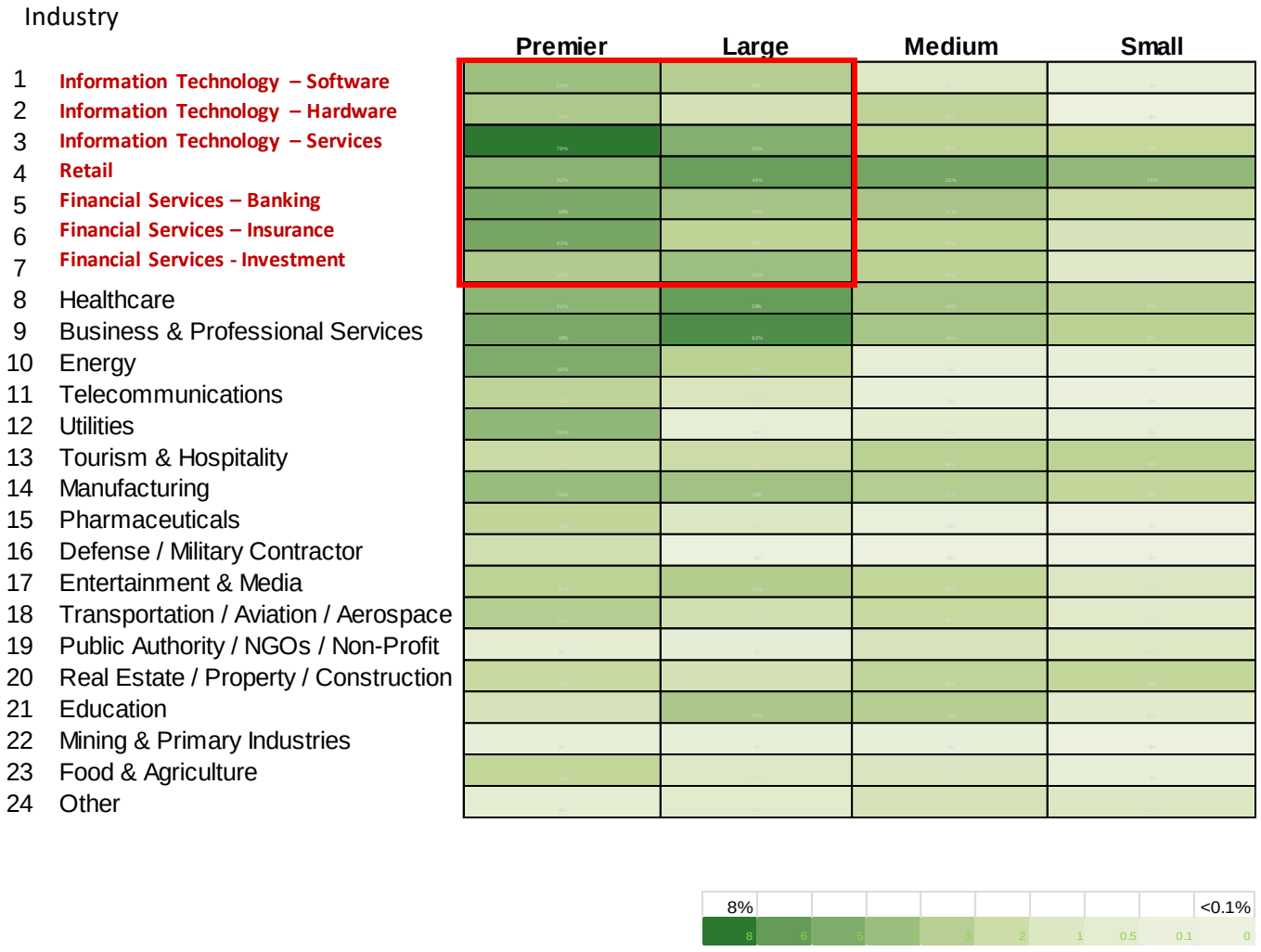
Affirmative

- You sell the policy for it
- You want some losses
- Yet you want to choose so you don't have too many losses
- You want to be sure of your limits
- You want to be sure of your clauses

Silent

- You didn't price the risk, but it is hidden in your policies
- Asbestos is the great example
- Hit *all lines*
- Is silent cyber similar?
- We better start pricing and selling it then
- (The greatest trick I ever played)

Can you Differentiate Cyber Risk?



- 6,838 companies in the 14 cells of highest priority
- Currently responsible for around 30% of the premium of the total US cyber affirmative insurance market
- Also projected as a key area of demand for higher limits and extended coverage
- Captures the leading players in the cyber economy

The testbed could potentially be expanded

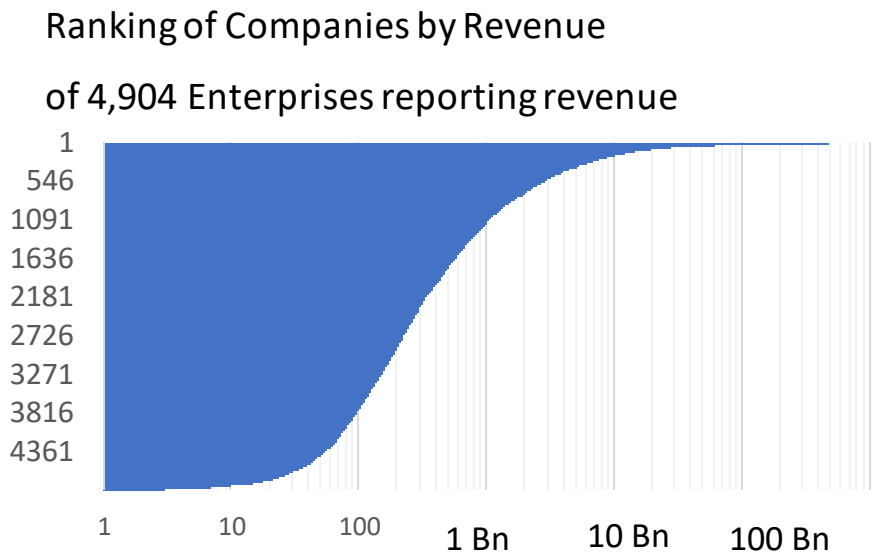
- to cover medium and small companies in these sectors
- to all other sectors and sizes in US
- to similar company lists in other jurisdictions

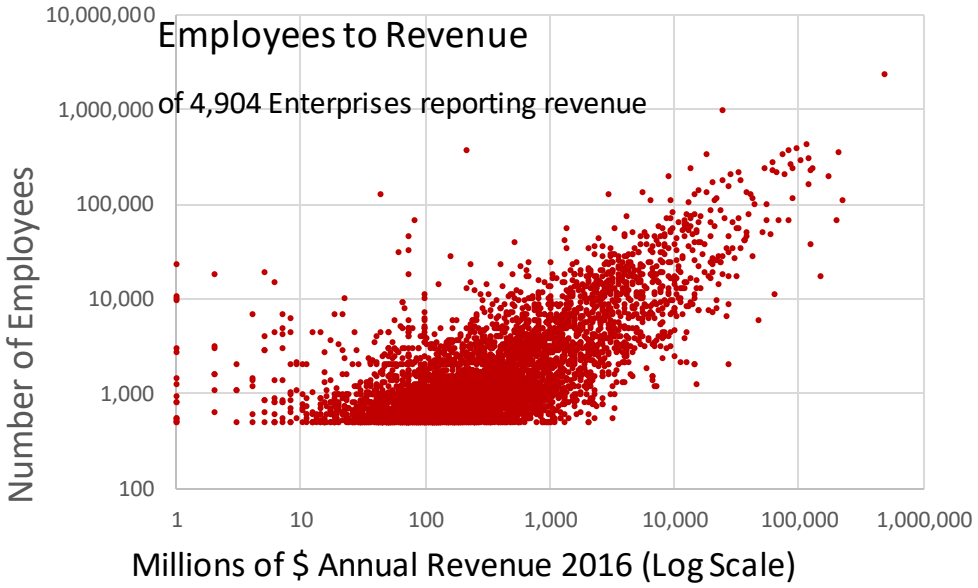
US Company inventory

U.S.		Premier	Large	Medium	Small	All	% of total
	Number of Employees:	>2,000	500-1,999	100-499	20-99		
	Revenue:	>$3 Bn	$40m-$3Bn	$10m-$40m	$2m-$20m		
	Ave Annual Revenue:	$14 Bn	$240 m	$28 m	$11 m		
Business Sector							
Information Technology - Software		11	55	267	1,046	**1,379**	0.2%
Information Technology - Hardware		12	14	61	168	**255**	0.0%
Information Technology - Services		32	395	1,897	7,507	**9,831**	1.6%
Retail		177	2,177	12,645	80,486	**95,485**	16.0%
Financial Services - Banking		44	277	2,201	6,238	**8,760**	1.5%
Financial Services - Insurance		70	254	976	4,061	**5,361**	0.9%
Financial Services - Investment Management		52	205	2,201	2,362	**4,820**	0.8%
Healthcare		47	2,877	15,654	61,702	**80,280**	13.4%
Business & Professional Services		49	4,473	15,757	60,704	**80,983**	13.6%
Energy		58	27	338	1,838	**2,261**	0.4%
Telecommunications		13	43	221	1,013	**1,290**	0.2%
Utilities		89	94	527	2,986	**3,696**	0.6%
Tourism & Hospitality		27	681	6,292	87,155	**94,155**	15.8%
Manufacturing		285	2,119	8,805	40,876	**52,085**	8.7%
Pharmaceuticals		23	34	136	354	**547**	0.1%
Defense / Military Contractor		2	25	27	124	**178**	0.0%
Entertainment & Media		37	407	2,528	15,385	**18,357**	3.1%
Transportation / Aviation / Aerospace		43	896	2,937	13,985	**17,861**	3.0%
Public Authority / NGOs / Non-Profit		0	215	1,558	18,562	**20,335**	3.4%
Real Estate / Property / Construction		28	813	5,592	48,516	**54,949**	9.2%
Education		16	387	2,398	13,372	**16,173**	2.7%
Mining & Primary Industries		4	81	236	759	**1,080**	0.2%
Food & Agriculture		56	283	1,210	5,295	**6,844**	1.1%
Other		0	215	1,558	18,562	**20,335**	3.4%
All		**1,173**	**17,047**	**86,021**	**493,056**	**597,297**	
		0.2%	2.9%	14.4%	82.5%		

Enterprise Database

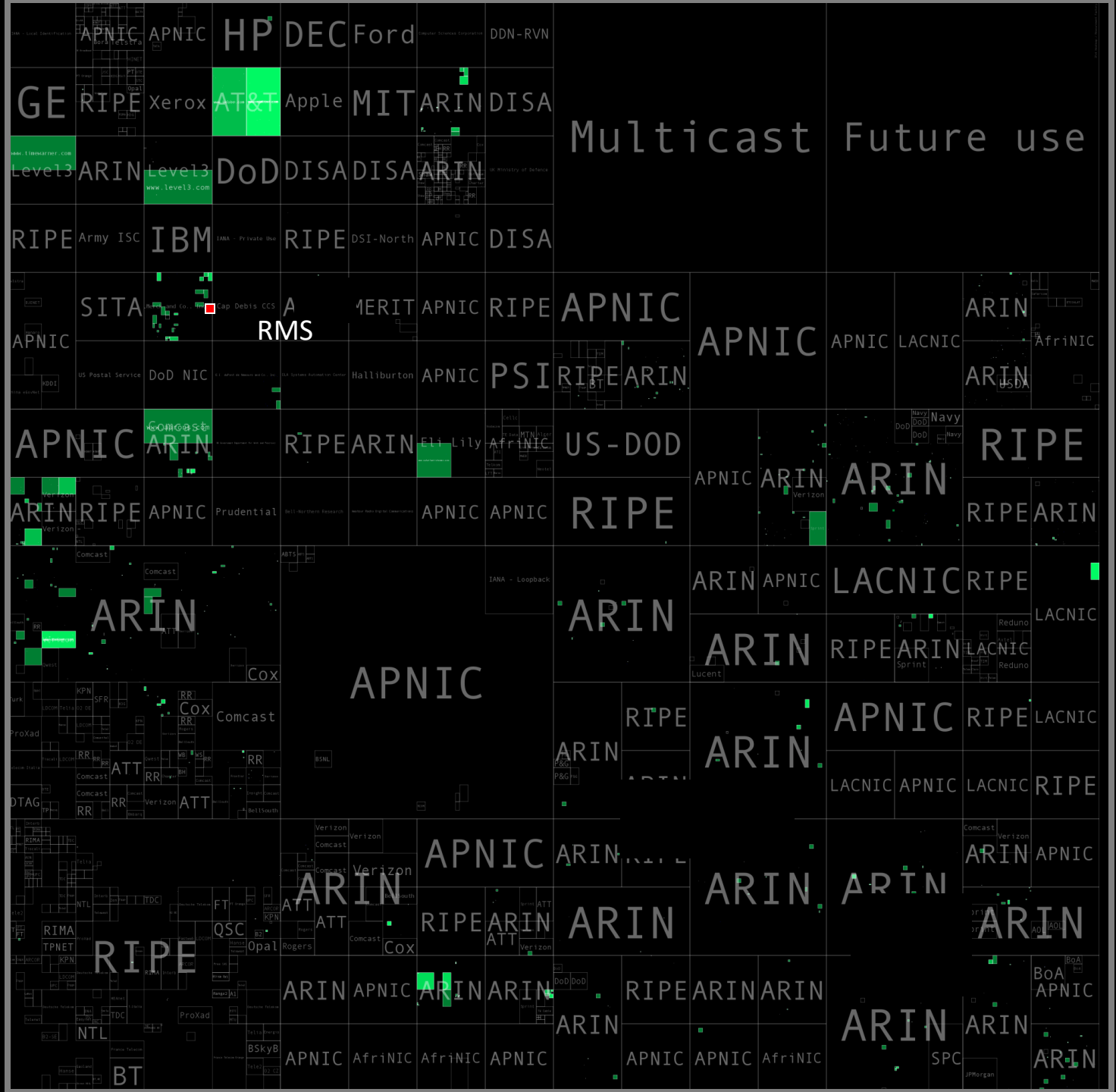
- Private companies of 500 employees or more in US economy
- Companies classified as being in sectors IT, Financial Services, Retail
- 6,839 Organizations
  - 3,479 “Operating”
  - 3,359 “Operating Subsidiary”
- All companies report no. of employees
- Only 4,904 (72%) report revenue
  - Operating: 2,618 report revenue (75%)
  - Subsidiary: 2,303 report rev (68%)
- Estimated total of **$10.7 Trillion** of revenue
  - Making assumptions about companies not reporting revenues
- Total reported profit: **$2.2 Trillion**
  - 12% of US GDP 2016



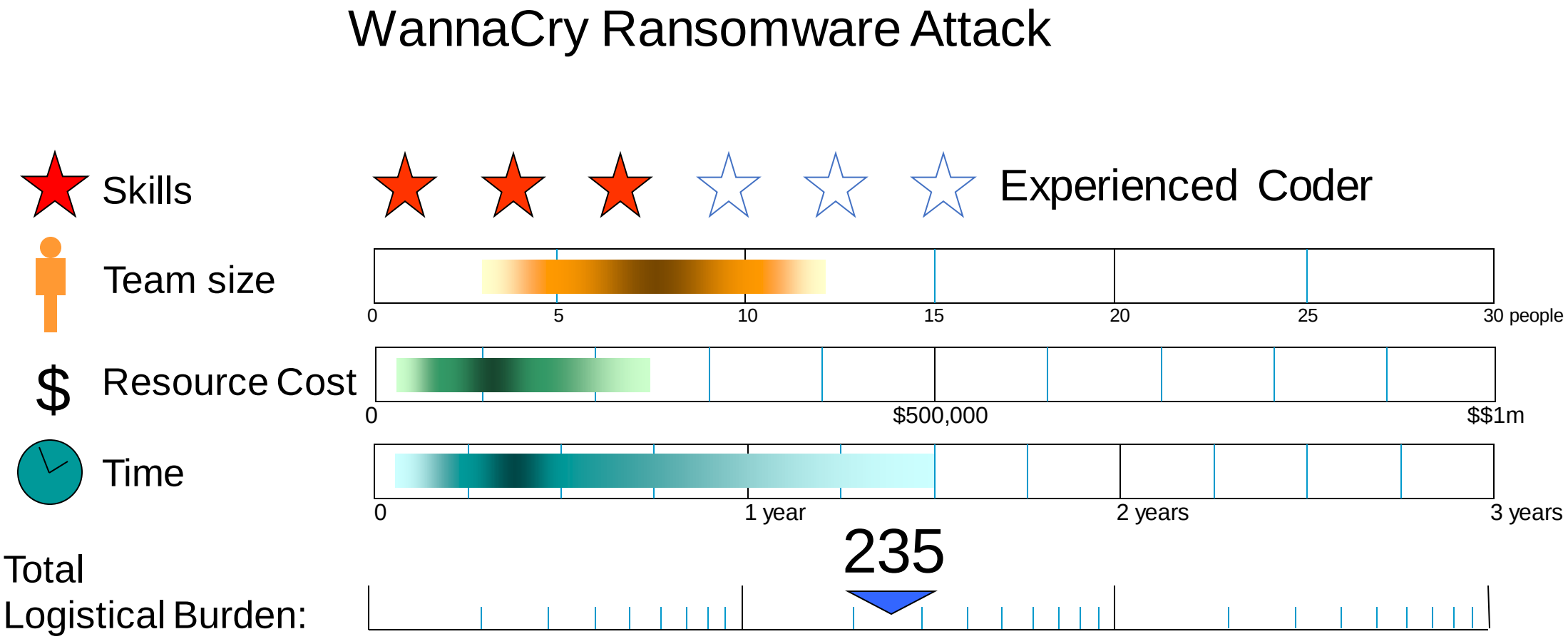


Locating companies in cyber space

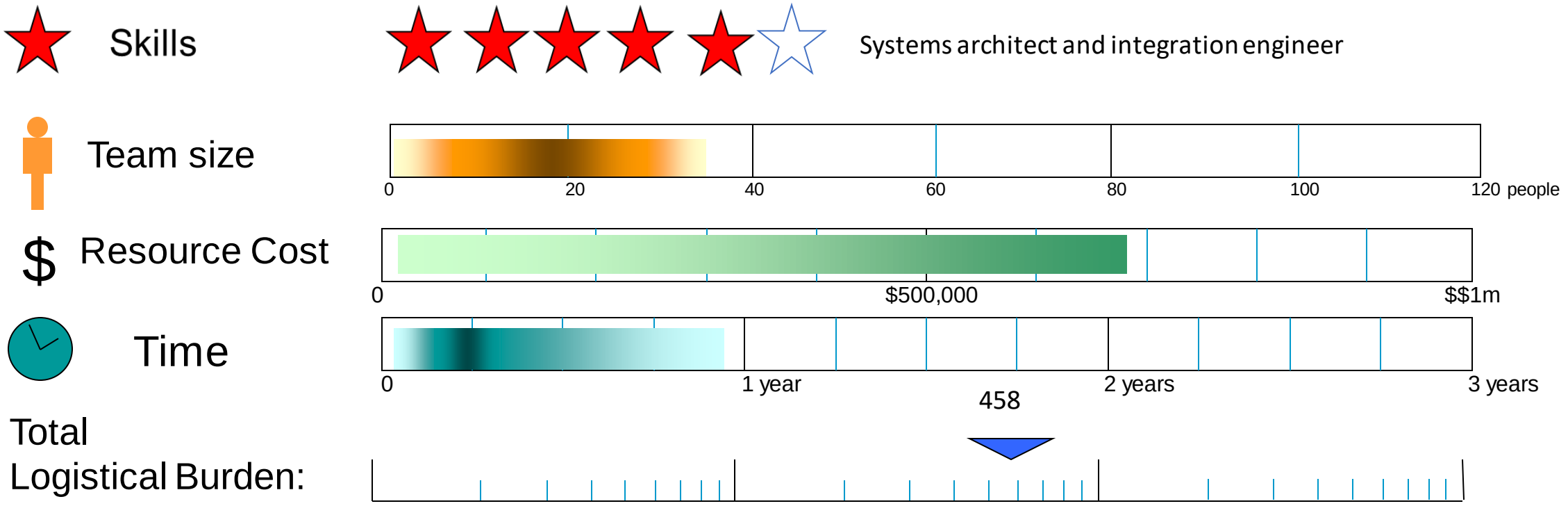
- All Fortune 100 companies plotted by their IPv4 domain address
- Working on developing a plot of IP addresses from enterprise database



Logistical burden for a cyber campaign

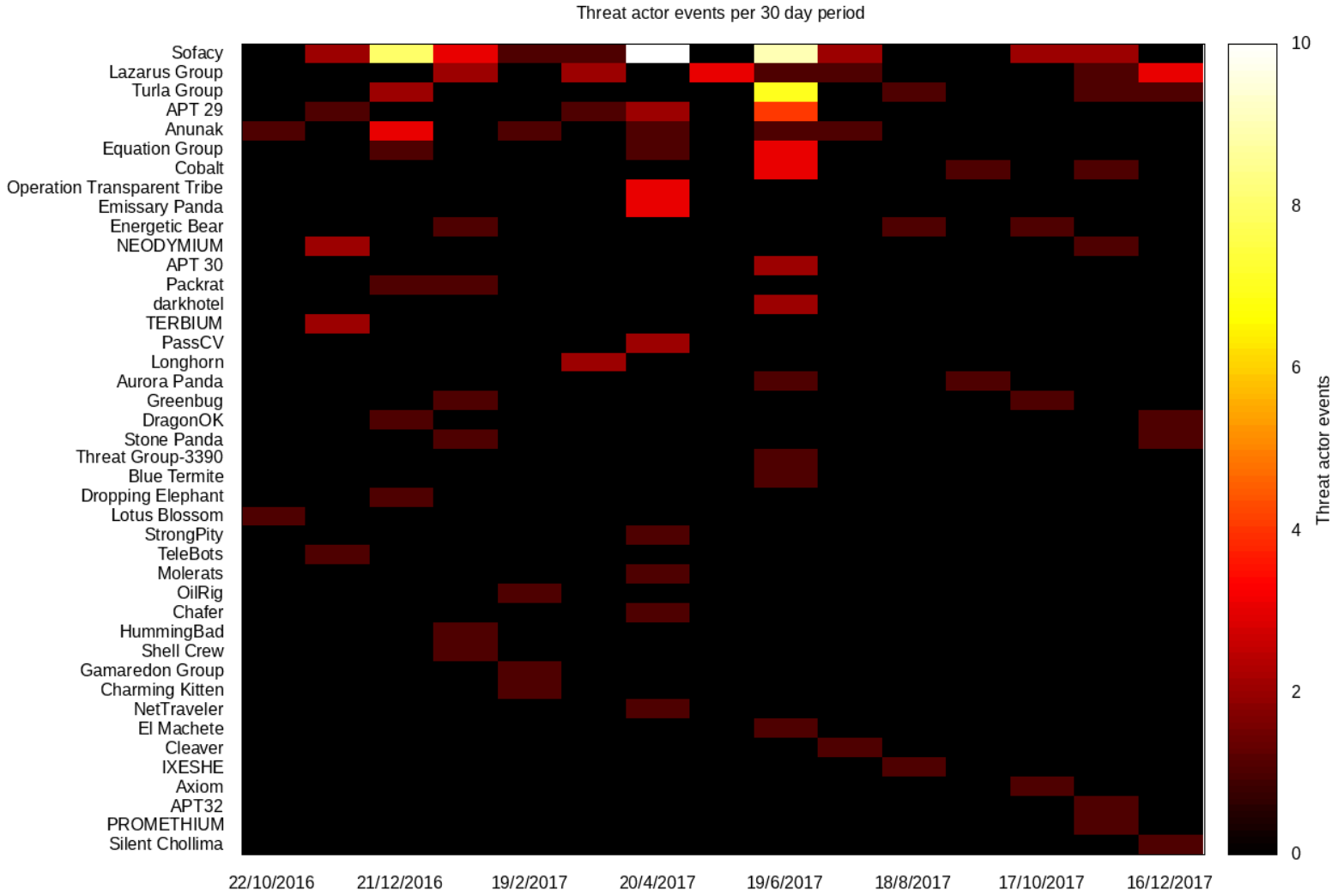


Logistical burden for a cyber campaign: Watering-hole attack



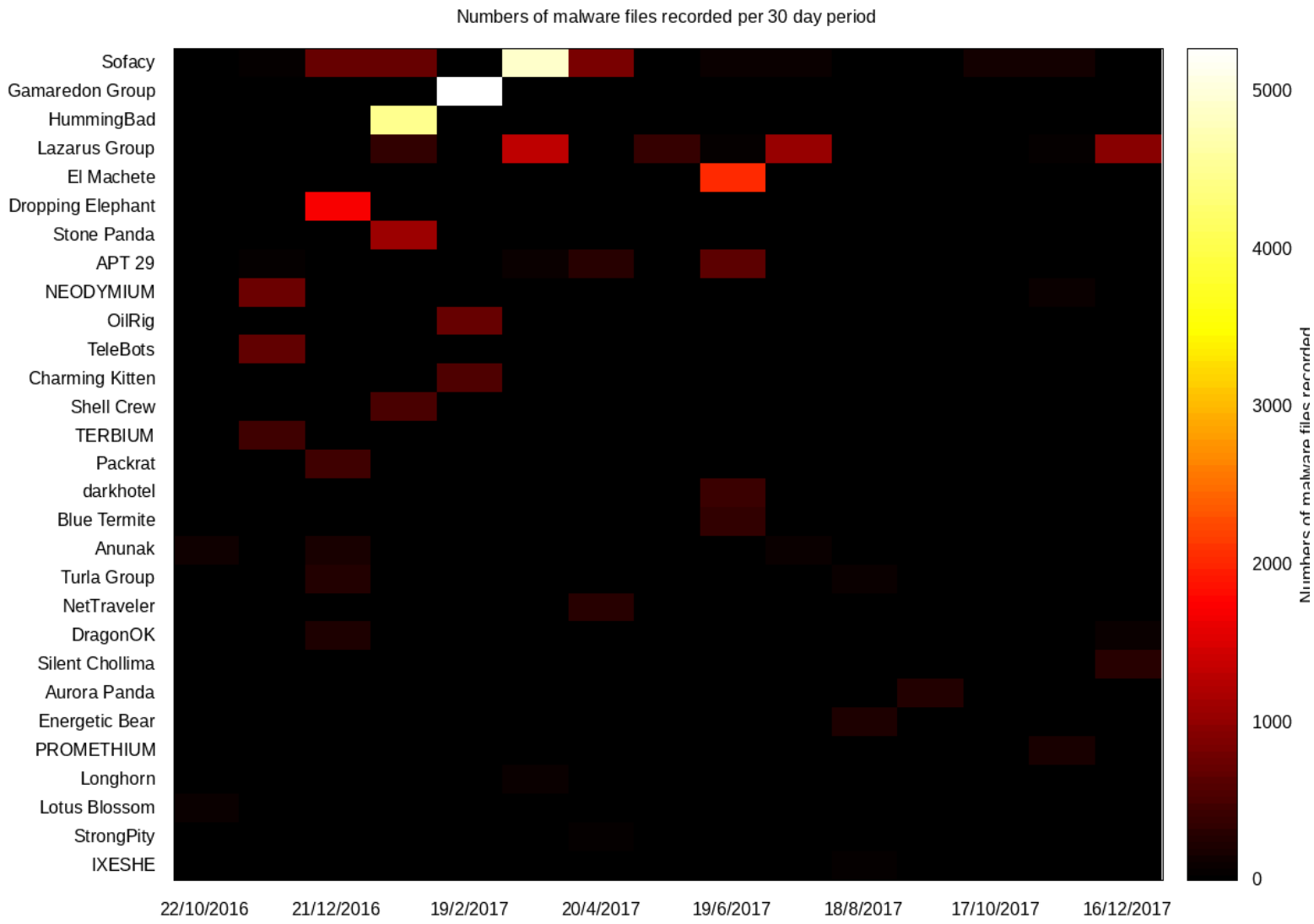
Relative Logistical Burden of Different Cyber Attacks

	Skill Level	Team Size	Cost	Months	Team Cost per Month	Team Cost	Total Cost Logistical Burden Index
Financial Transaction Theft - Upper Stress Test	STOL	60	1,000,000	24	200,000	4,800,000	**5,800,000**
Financial Transaction Theft - Reference	STOL	48	750,000	18	150,000	2,700,000	**3,450,000**
Leakomania - Upper Stress Test	STOL	30	500,000	12	146,000	1,752,000	**2,252,000**
Financial Transaction Theft - Lower Stress Test	Systems Architect	36	500,000	12	100,000	1,200,000	**1,700,000**
Mass DDoS - Upper Stress Test	Systems Architect	12	500,000	12	90,000	1,080,000	**1,580,000**
Mass DDoS - Reference View	Systems Architect	8	300,000	9	90,000	810,000	**1,110,000**
Watering-hole Attack	Systems Architect	33	450,000	11	80,000	880,000	**1,330,000**
Leakomania - Reference View	Systems Architect	25	250,000	9	90,000	810,000	**1,060,000**
Extortion Spree - Upper Stress Test	Systems Architect	20	250,000	12	50,000	600,000	**850,000**
Mass DDoS - Lower Stress Test	Systems Architect	6	200,000	6	90,000	540,000	**740,000**
Leakomania - Lower Stress Test	Highly Experienced Coder	16	200,000	8	32,000	256,000	**456,000**
Extortion Spree - Reference View	Highly Experienced Coder	16	150,000	8	32,000	256,000	**406,000**
Extortion Spree - Lower Stress Test	Experienced Coder	12	90,000	6	24,000	144,000	**234,000**
WannaCry Ransomware Attack	Experienced Coder	8	50,000	6	23,000	138,000	**188,000**



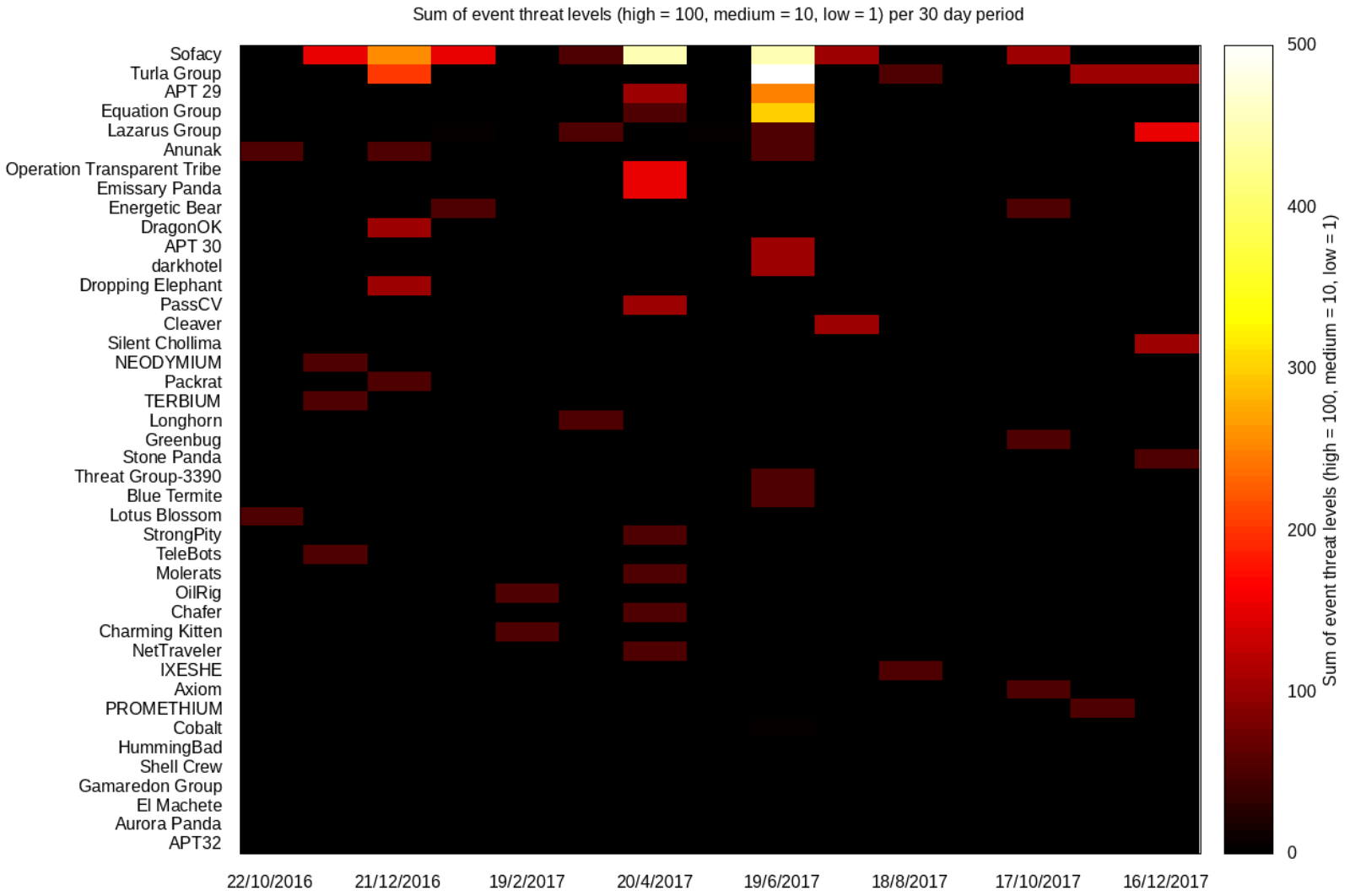
From Theory to Practice

Binaries per APT

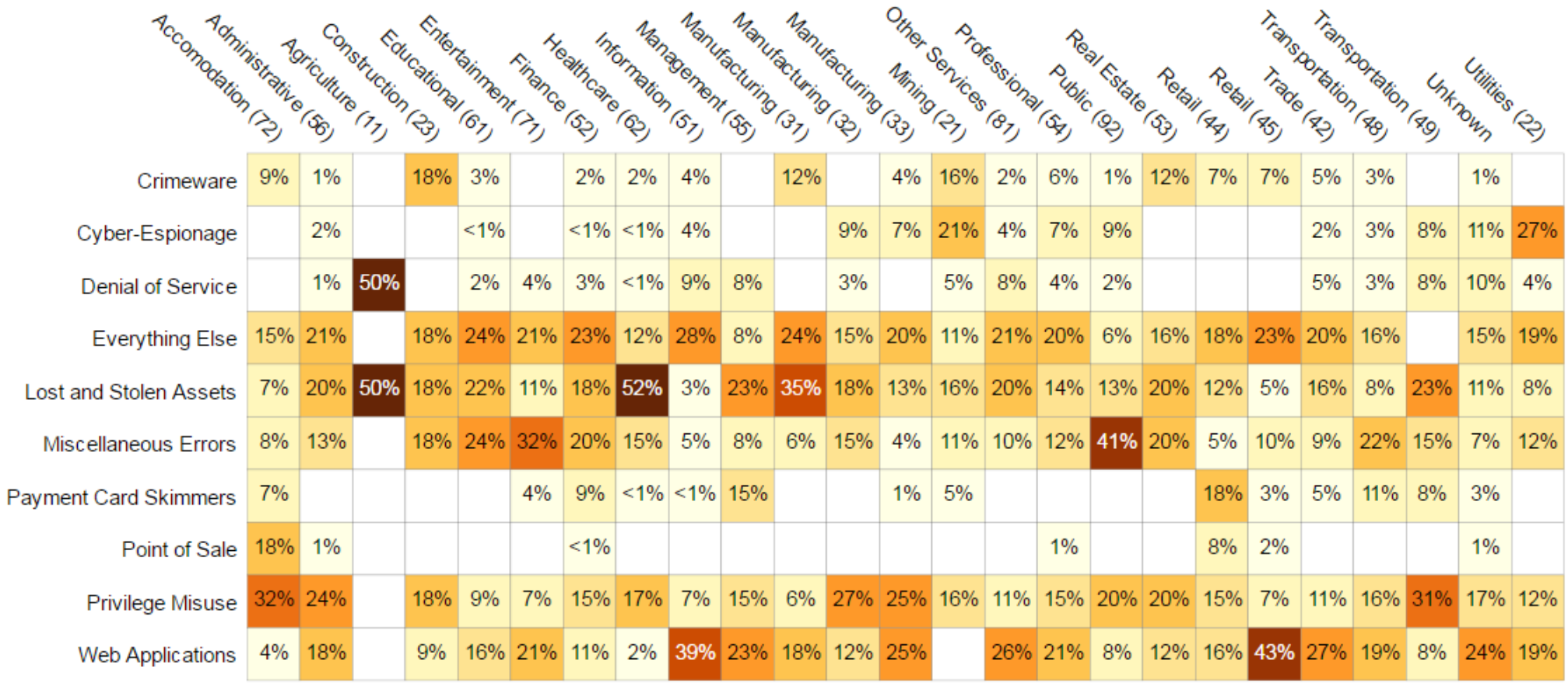


Multi-dimension burden scoring:

- Network address (Source and Destination)
- Malicious URLS
- Binaries
- Events



VCDB Incident/Breach Patterns By Industry



	Accomodation (72)	Administrative (56)	Agriculture (11)	Construction (23)	Educational (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Management (55)	Manufacturing (31)	Manufacturing (32)	Manufacturing (33)	Mining (21)	Other Services (81)	Professional (54)	Public (92)	Real Estate (53)	Retail (44)	Retail (45)	Trade (42)	Transportation (48)	Transportation (49)	Unknown	Utilities (22)
Crimeware	9%	1%		18%	3%		2%	2%	4%		12%		4%	16%	2%	6%	1%	12%	7%	7%	5%	3%		1%	
Cyber-Espionage		2%			<1%		<1%	<1%	4%			9%	7%	21%	4%	7%	9%				2%	3%	8%	11%	27%
Denial of Service		1%	50%		2%	4%	3%	<1%	9%	8%		3%		5%	8%	4%	2%				5%	3%	8%	10%	4%
Everything Else	15%	21%		18%	24%	21%	23%	12%	28%	8%	24%	15%	20%	11%	21%	20%	6%	16%	18%	23%	20%	16%		15%	19%
Lost and Stolen Assets	7%	20%	50%	18%	22%	11%	18%	52%	3%	23%	35%	18%	13%	16%	20%	14%	13%	20%	12%	5%	16%	8%	23%	11%	8%
Miscellaneous Errors	8%	13%		18%	24%	32%	20%	15%	5%	8%	6%	15%	4%	11%	10%	12%	41%	20%	5%	10%	9%	22%	15%	7%	12%
Payment Card Skimmers	7%					4%	9%	<1%	<1%	15%			1%	5%					18%	3%	5%	11%	8%	3%	
Point of Sale	18%	1%					<1%									1%			8%	2%				1%	
Privilege Misuse	32%	24%		18%	9%	7%	15%	17%	7%	15%	6%	27%	25%	16%	11%	15%	20%	20%	15%	7%	11%	16%	31%	17%	12%
Web Applications	4%	18%		9%	16%	21%	11%	2%	39%	23%	18%	12%	25%		26%	21%	8%	12%	16%	43%	27%	19%	8%	24%	19%

108.49 Tb/s

Regional

Via Protocol

IoT: Is it a product or a service?

Product Liability

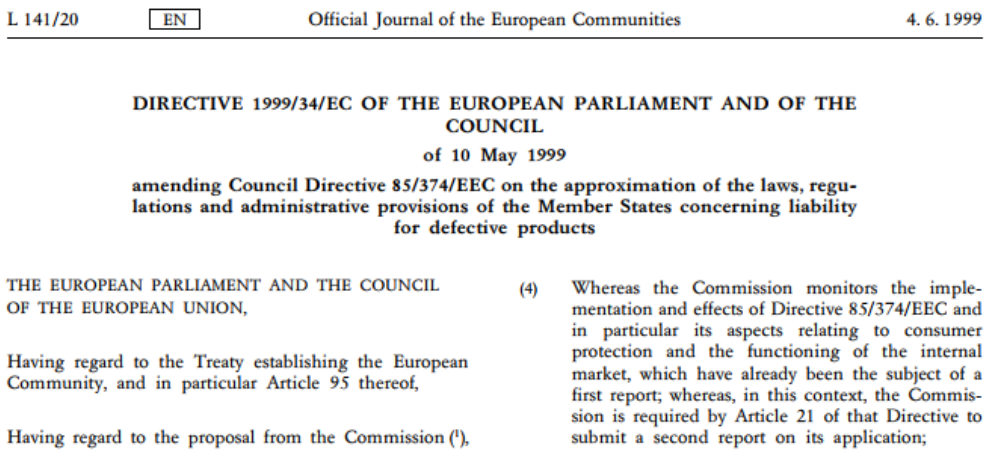
- If a dishwasher floods a kitchen
- If a washing machine overheats
- If a phone catches fire
- If toys are choke hazards
- Recognises differences between defects:
  - Design
  - Manufacturer
  - Informed misuse
- Shared/proportional liability

Firmware/Service Non-Liability

- EULA
- Assumed non-liable
  - For defects
  - For vulnerabilities
  - For exploits

EU Product Liability Directive

- Article 12
- The liability of the producer arising from this Directive may not, in relation to the injured person, be limited or excluded by a provision limiting his liability or exempting him from liability.



L 141/20 EN Official Journal of the European Communities 4. 6. 1999

DIRECTIVE 1999/34/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 10 May 1999

amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

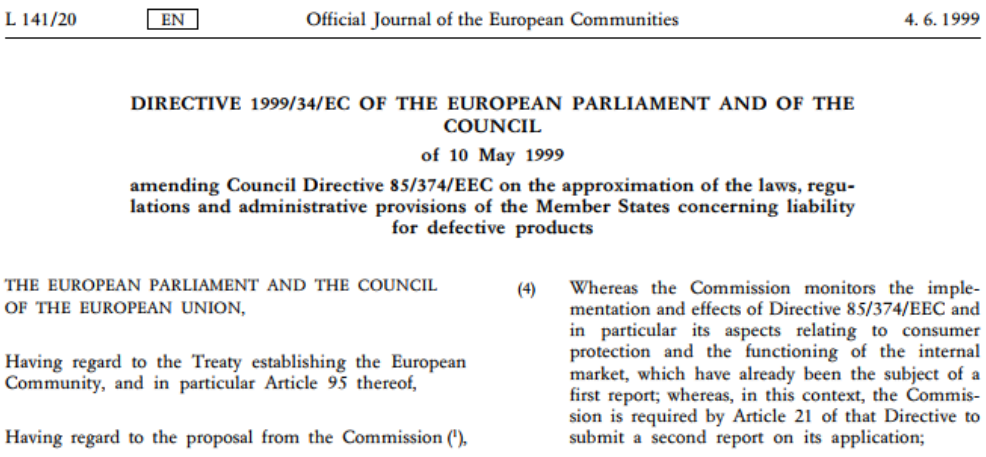
Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

(4) Whereas the Commission monitors the implementation and effects of Directive 85/374/EEC and in particular its aspects relating to consumer protection and the functioning of the internal market, which have already been the subject of a first report; whereas, in this context, the Commission is required by Article 21 of that Directive to submit a second report on its application;

EU Product Liability Directive

- Article 8
- 1. Without prejudice to the provisions of national law concerning the right of contribution or recourse, the liability of the producer shall not be reduced when the damage is caused both by a defect in product and by the act or omission of a third party.
- 2. The liability of the producer may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person or any person for whom the injured person is responsible.



L 141/20 EN Official Journal of the European Communities 4. 6. 1999

DIRECTIVE 1999/34/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 10 May 1999

amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission (1),

(4) Whereas the Commission monitors the implementation and effects of Directive 85/374/EEC and in particular its aspects relating to consumer protection and the functioning of the internal market, which have already been the subject of a first report; whereas, in this context, the Commission is required by Article 21 of that Directive to submit a second report on its application;

Lots of R&D opportunity in cyber risk

Selling insurance is boring...

CREATING it is epic!

Watch out for our book: Solving Cyber Risks

In 2019

by

Dr Andrew Coburn, Mr Eireann Leverett, Dr Gordon Woo

@blackswanburst