UC RIVERSIDE

OEM: Weekly SITREP

April 12, 2022

UC RIVERSIDE Office of Emergency Management

USA & WORLD

- With COVID mission over, Pentagon plans for next pandemic.
- Chinese hackers launch cyberattacks against Ukraine amid war.
- Biden & EU risk nuclear war unless Putin given an off ramp.
- Chinese hackers reportedly target India's power grid.
- Particle experiment could spark physics revolution.
- Financial fraud shot up 233% last year.
- Student suspended for handing out fentanyl-laced candy.
- Are tech companies removing evidence of war crimes?
- Study of gun injuries quantifies the impacts on survivors & families.
- Wastewater monitoring for COVID-19 is growing across the U.S.
- Tragic Ukraine story told with drones, satellites and social media.
- How Ukraine has defended itself against cyberattacks.
- What's next for defending critical infrastructure?
- NSA employee accused of sharing national defense secrets.
- iOS 15.4.1—"Update now" warning issued to all iPhone users.
- Russia's Crypto: Rubles for enemies and Bitcoin for friends.
- Google issues warning to those who dismiss Russia-Ukraine war.
- Russia's slow cyberwar in Ukraine begins to escalate, experts say.
- JPMorgan CEO: dramatic increase of risks ahead for U.S.

UC RIVERSIDE Office of Emergency Management

New report details ten different hacking operations which are known to have actively targeted industrial systems in North America and Europe – and it's warned that this activity is likely to grow in the next 12 months.

- **Parasite**: a group which targets utilities, aerospace and oil and gas in Europe, the Middle East and North America. Thee group uses open source tools and known vulnerabilities for initial access. Parasite is suspected to be linked to Iran.
- **Xenotime**: a group which targets oil & gas companies in Europe, the United States and Australia. It's believed the group is linked to Russia.
- **Magnallium**: a group which initially targeted oil and gas and aircract companies in Saudi Arabia, which has expanded targeted to Europe and North America. It's thought to be related to APT 33, a state-sponsored Iranian hacking group.
- **Dymalloy**: a group which targets electric utilities, oil and gas and other advanced industrial entities across Europe, Turkey and North America. Described as "highly aggressive", Dymalloy looks for long-term persistence in networks and is thought to be linked to Russia.
- **Electrum**: this group is capable of developing malware that can modify and control OT procedures and Dragos researchers say this operation was responsible for Crash Override – also known as Industroyer – a malware attack on Ukraine's power grid in December 2016. Electrum is associated with Sandworm, an offensive hacking operation that's part of Russia's GRU military intelligence agency.
- **Allanite**: a group which targets enterprise and OT networks in the UK and US elecricity sectors, as well as German industrial infrastructure and uses access to conduct reconnaissance on networks to potentially stage future disruptive events. It's believed Allanite is linked to Russia.
- **Chrysene**: Active since at least 2017, this group has targeted industrial organisations in Europe and the Middle East, and mainly conducts intelligence gathering operations to potentially facilitate further attacks. Chrysense is suspected to be linked to Iran.
- **Kamacite**: a group which has been active since at least 2014 and believed to be responsible for cyber attacks against Ukrainian power facilities in 2015 and 2016. The group is linked to Sandworm.
- **Covellite**: a group which has targeted electric utilities in Europe, the US and East Asia using malicious attachments in phishing emails. The group is thought to be linked to the Lazarus Group, a state-backed hacking group working out of North Korea.
- **Vanadinite**: A hacking group which targets external-facing, vulnerable software in industrial organisations around the world. It's thought to be linked to APT 41, a state-sponsored Chinese hacking operation.

CALIFORNIA

- California oil and gas production is the only way forward.
- More than 4K Stanford nurses vote to strike.
- Drought could disrupt hydropower electricity generation this summer.
- Man who tried to join ISIS sentenced to 20 years
- The Golden State's public schools are not doing their job.
- Statewide Health Information Exchange set to launch.
- Cities spent huge share of federal Covid relief funds on police.
- State gun restrictions are a failure.
- California eyes $100M cyber funding boost for community colleges.
- Why fining utility companies doesn't change a thing.
- Little snow remains - another sign of a dry and dangerous summer.
- State launches updated climate adaptation strategy.
- California labor law: how to sue employers.
- With students in turmoil, teachers train in mental health.
- UCB Crispr pioneer expects to see gene-edited babies within 25 years.
- Activist admits to launching DDoS attack against Santa Cruz County.
- California setting up statewide medical data-exchange grid.
- 20% of community college students report experiencing homelessness.
- State calling upon Native American tribes to do controlled burns.

Modernizing Our Behavioral Health Continuum: Sponsorship of Senate Bills to improve the behavioral health system.

SB 929

SB 929 will help us better understand the current state of our LPS system and how it cares for thousands of vulnerable Californians. This bill will provide information that will help evaluate the services and strategies currently utilized, and allow the state to improve outcomes for those who are served.

SB 965

We continue to see the struggles of our community members that cycle in and out of hospitalizations, shelters, and jails without getting the concrete connections to needed medication and treatment. We are encouraging support of SB 965 to ensure that relevant history can be considered by the court in a uniform manner across the state. Tools focused on acute symptoms are not suited for chronic and severe conditions that we see on our streets. This bill will ensure that a complete and accurate picture is presented in court when considering the very serious step of conservatorship.

SB 970

The Mental Health Services Act has been a crucial, dedicated funding mechanism for community behavioral health services for the last 15-plus years, and we are excited to support the continuous improvement of the Act through SB 970. Though the Act has served as an incredible tool to build up community-based services, we feel that a more direct focus on service outcomes, increased transparency and accountability, and frequent progress reports will help improve service delivery that our communities rely on.

SB 1035

Assisted Outpatient Treatment has long been an effective, if underutilized, tool for providing appropriate and intensive outpatient treatment to Californians that have been repeatedly hospitalized or have come into contact with law enforcement due to their serious mental illness. While SB 1035 can be characterized as a clarification, we feel it is important to ensure that there is no ambiguity on the ability to include self-administered medication in a court-ordered treatment plan. Medication may not be a cure-all for the conditions faced by many in our community, but it is a key component of long-term recovery.

SB 1227

Current law allows for a gravely disabled person receiving 14 days of intensive treatment to be certified for an additional 30 days. Continuing the goal of most of the bills in this package to reduce the need for additional conservatorships, SB 1227 would allow for a single 30-day extension of the existing option for 30-day intensive treatment. Our hope is that an additional 30 days to recover and reconstitute can reduce the need for conservatorship.

SB 1238

As we have seen with our struggles with housing and homelessness, people frequently cross city and county lines seeking shelter, community, and treatment. Despite the state's view of these issues as regional in nature, behavioral health needs are not viewed in the same way. SB 1238 would establish a regional planning process to evaluate whether behavioral health services and infrastructure are meeting the needs we have today and identify the needs that we should be planning for in the future.

REGION

- Thousands rally in LA to oppose COVID-19 vaccine mandates.
- 42 million gallons of sewage entered L.A. waterways in past 15 years.
- Jury to decide USC coach's fate in college bribery trial.
- Protesters arrested after chaining themselves to bank entrance.
- International burglary rings lead to spike in crime in SoCal.
- SpaceX: First-of-its-kind launch to the International Space Station.
- LA man pleads guilty to interfering with flight crew.
- South LA gang leader called 'boss of bosses' at start of racketeering trial.
- Sacramento shooting suspect wanted in Riverside County since 2015.
- 'Unspoken pandemic': Fentanyl overdoses in SoCal.
- BLM purchased $6 Million house in SoCal with non-profit donations.
- Metrolink adds 26 trains to its schedule as ridership bounces back.
- Volunteers sought for RivCo's Emergency Animal Rescue Program.
- Hot air balloon crashes in Riverside County.
- L.A. ranks as one of the deadliest cities for rappers.
- Judge orders LA sheriff to testify about deputy gangs.
- Museum of Riverside receives 19k award to help Native culture.

Are Firefighters Hard to Recruit?

In response to a recent California Policy Center analysis that provided an updated calculation of the average pay and benefits for full-time firefighters working for cities in California, one commenter claimed that it has become difficult to recruit firefighters.

Firefighter Compensation in California Cities
25 Largest Departments
2020, $ = 000

UAAL = Unfunded Actuarial Liability,
yellow highlighted are cities that included UAAL
in the amount of the employer pension payment

Agency	Base Pay	OT Pay	Other Pay	Total Pay	Pension	Health Ins.	Total Benefits	Total Comp
Average All Cities	115	46	12	173	38	17	54	227
Avg UAAL Included	123	50	10	183	52	17	69	252
Avg UAAL Not Incl.	108	42	14	164	26	17	43	207
Santa Clara	172	33	34	240	100	12	112	352
Oakland	124	51	14	190	66	21	87	276
Los Angeles	125	63	3	190	57	16	73	263
Glendale	123	53	6	182	68	13	81	263
Berkeley	123	30	11	165	71	21	92	257
Ontario	125	54	23	202	25	21	46	248
Fremont	128	53	20	201	23	21	43	244
Pasadena	112	71	4	187	20	18	38	225
Torrance	83	50	51	184	25	16	41	225
San Jose	137	27	8	171	38	14	52	223
Riverside	106	51	21	178	32	11	44	221
Huntington Beach	104	47	28	179	25	15	40	219
Newport Beach	113	50	16	179	24	16	40	218
San Francisco	125	26	18	169	29	-	47	216
Long Beach	117	55	3	174	24	16	40	214
Anaheim	121	47	8	176	-	18	38	214
Stockton	85	35	12	132	57	11	68	201
Chula Vista	96	53	12	161	22	15	37	198
Sacramento	110	33	2	145	24	16	40	185
Modesto	97	44	14	155	18	4	22	177
Bakersfield	87	27	15	130	24	16	40	170
Fresno	96	28	8	131	20	15	35	166
San Diego	73	29	16	118	15	14	29	147

The County of Riverside Emergency Operations Center is currently activated to Management Watch.

COMMUNICATIONS

- 11 April:
  - School of Medicine Online Open House
- 8 April :
  - First VCUA Candidate Vision Seminar – Tuesday, April 12th
- 7 April :
  - UCR Ecologists study how mountain streams signal climate change
- 6 April :
  - New Face Covering Guidelines Take Effect April 11
  - Register: UC Cyber Security Summit Online – April 20
  - Associate Vice Chancellor of Enrollment Services

Please Reference Notes Section For More Information

NOTABLE

- When It Comes To Cyber Risk, You're Only As Safe As Your Vendors
- Battling Cybersecurity Risk: How to Start Somewhere, Right Now
- Cyber risk now tops concerns among companies
- Europe Warned About Cyber Threat to Industrial Infrastructure
- The anatomy of cyber risk
- A Comprehensive Guide to Cyber Risk Quantification
- What is Cyber Risk Quantification? An Analysis of Financial Impact
- The cyber risk self-insurance challenge for corporate boards
- Cyber risk: Why we need a new approach to handling this explosive threat
- Harvard Law School: Overseeing Cyber Risk
- Why Supply Chains Are Entering Third Year of Chaos: QuickTake
- The metaverse may bring new cyber risks. Here’s what companies can do
- Insurable or not insurable? The new questions surrounding cyber risk insurance
- Top 10 Considerations in Cybersecurity Risk Management
- Illinois Appellate Court Denies Business Interruption Insurance Claim Related to COVID-19
- Analysis: Cyber insurers face hefty Ukraine war-related claims, despite fine print
- How the invasion of Ukraine impacts the U.S. insurance industry
- 5 Ways Cyber Business Interruption Differs from Traditional Business Interruption
- Cyber the next battle line for your business
- Russia War Raises Global Insurers' Cyber Claim Exposure

Cyber Risk

UC RIVERSIDE Office of Emergency Management

- Cyber risk poses serious threats for businesses around the world.
- Cyber risk management is no longer just about preventing breaches.
- The threat environment is becoming more complex with an increasing number of threat actors, including nation states, using new and more sophisticated tactics.

> The cyber risk buck ultimately stops with every company's boardroom and management team. The vast majority of the economic impacts of cyber risk cannot be insured away.

Figure 1 Global Cyber Risk Exposure Index

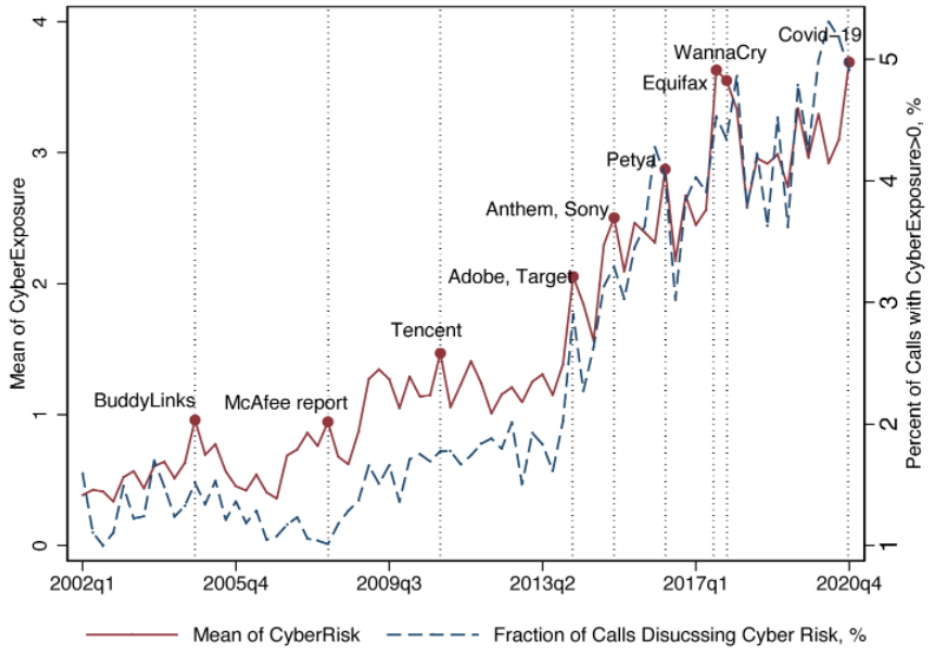
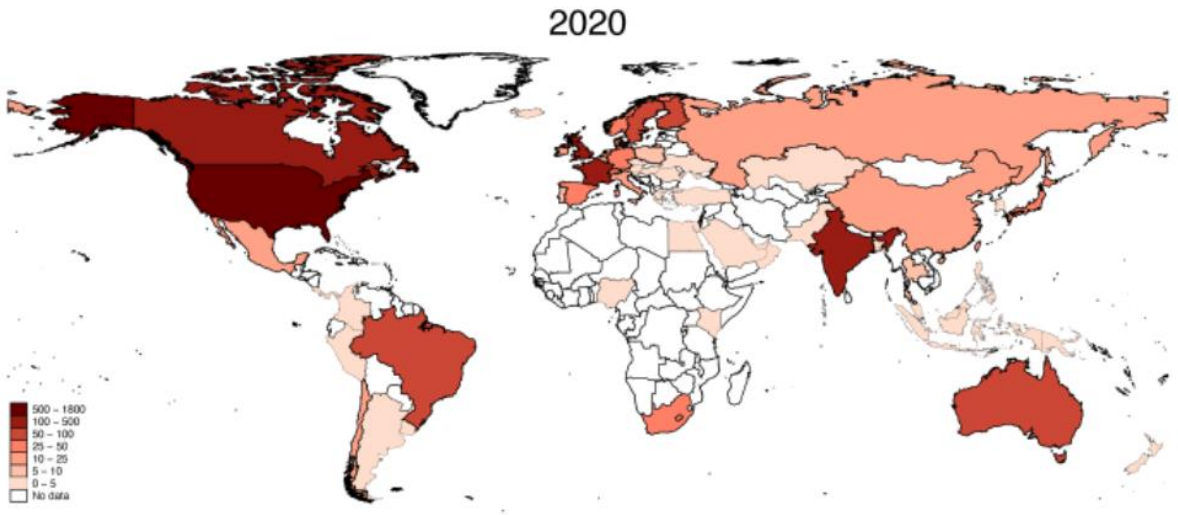
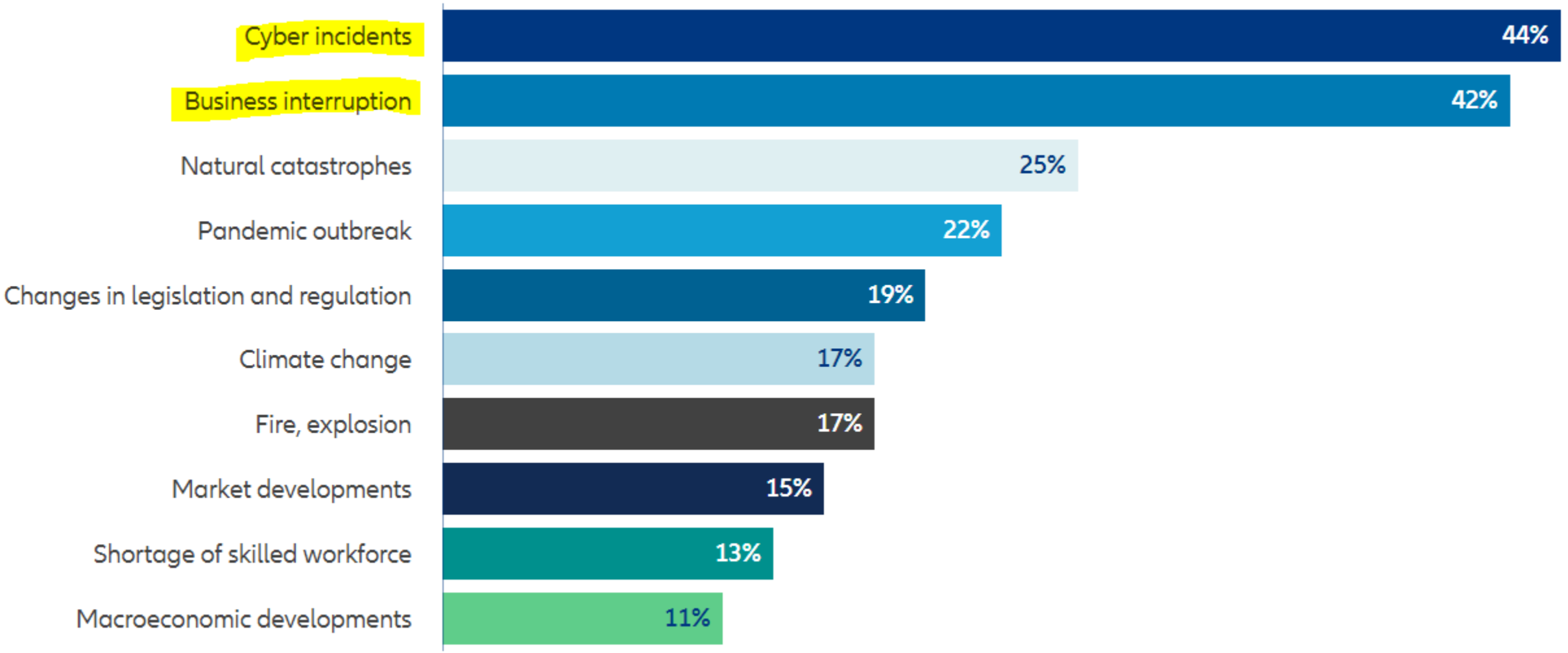


Figure 2 Global heatmap of cyber risk exposure



Global Business Risk 2022

UC RIVERSIDE Office of Emergency Management

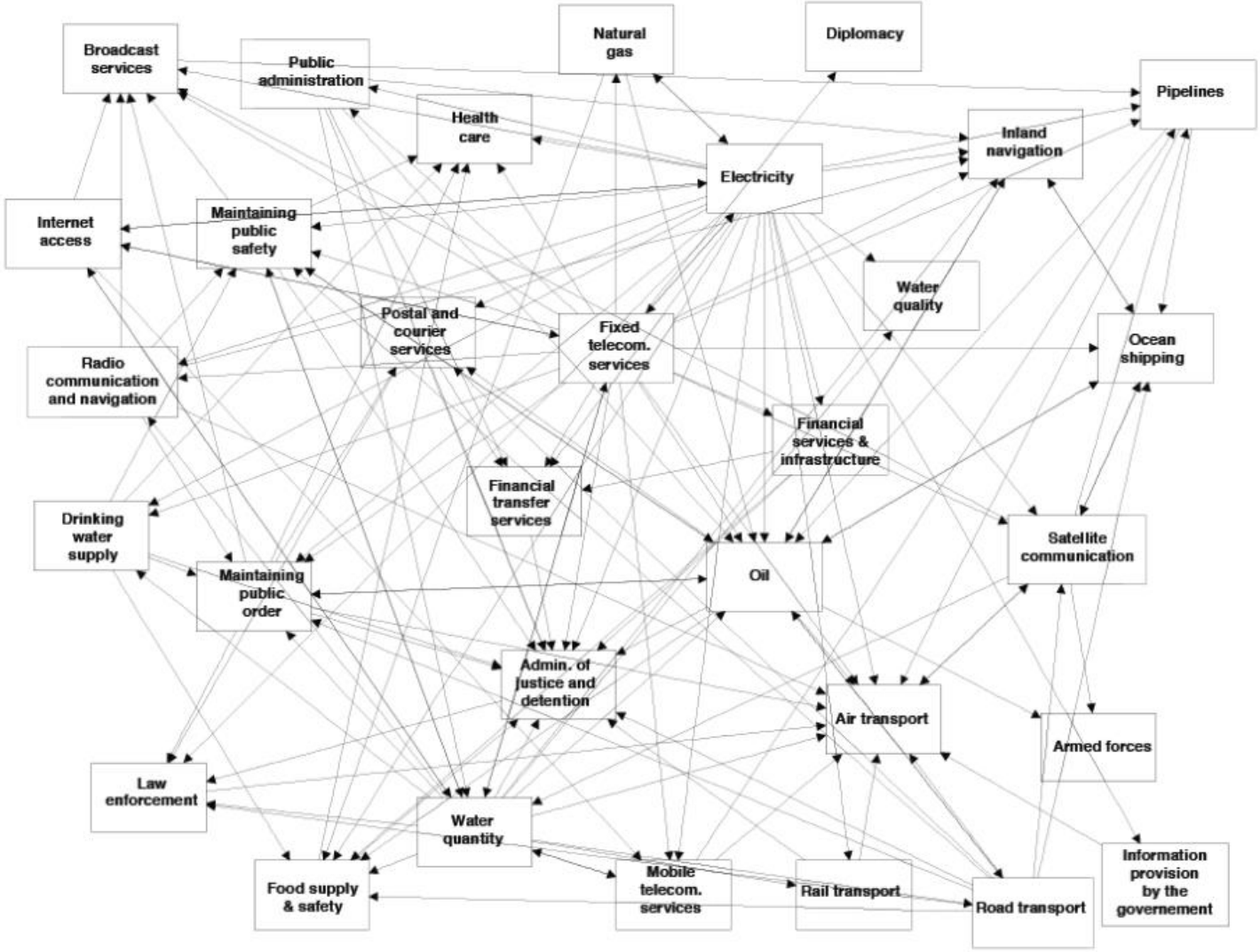


Systemic Cyber Risk & Interdependency

UC RIVERSIDE Office of Emergency Management

- There is growing concern about “systemic cyber risk”—the possibility that a single failure somewhere in cyberspace could cause widening ripples with catastrophic consequences.

- Whereas most cyber events have a narrowly defined set of victims, a systemic cyber incident could do damage on a national or even a global scale—threatening the digital infrastructure that entire societies, economies, and governments rely on to function.



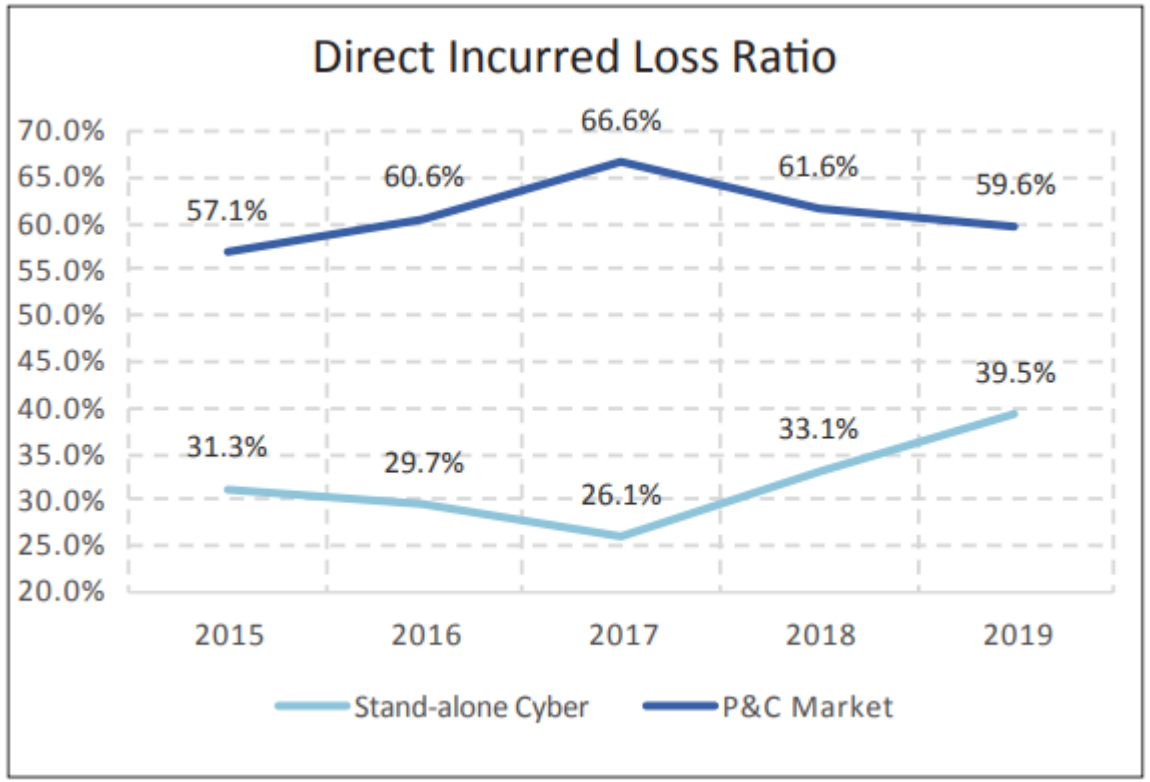
Various forms of interdependency—whether financial, biological, logistical, digital, or otherwise—can increase volatility in large-scale systems by boosting the chance that any given failure will spread, often in unexpected ways.

Cyber Risk: Market Outlook

- Despite the favorable loss ratio performance, the cyber insurance market is still relatively young, and its true claim cost is still uncertain since ***we have yet to observe a global market wide catastrophic insurance loss***.

- The recent substantial increase in cyberattacks and ransomware has increased the market wide loss ratios.

- Many industry professionals consider a cyber risk to be systemic if it is uninsurable—based on the scale of potential losses; loss correlation across many clients, sectors, and regions; and the difficulty of modeling and hedging.



Any events that generate massive correlated losses at a global scale—especially business interruptions, a major worry in systemic cyber events—will exceed the response capacity of the private insurance market.

Cyber Risk: Business Interruption

UC RIVERSIDE Office of Emergency Management

Business Interruption

Business interruption, also referred to as network interruption coverage, generally indemnifies the insured for business interruption loss, in excess of the retention, incurred by the insured during a period of restoration or extended interruption. To qualify the interruption should be a direct result of the actual and necessary interruption or suspension of computer systems that first takes place during the policy period and is directly caused by a failure of computer security to prevent a security breach. The security breach typically must first take place on or after the retroactive date and before the end of the policy period.

> If Russia carries out a large cyber attack which spills over into several countries, it could lead to claims totalling $20 billion or more, similar to insurance claims from a large U.S. hurricane, the industry sources said on condition of anonymity.

Cyber Risk: Business Interruption

UC RIVERSIDE Office of Emergency Management

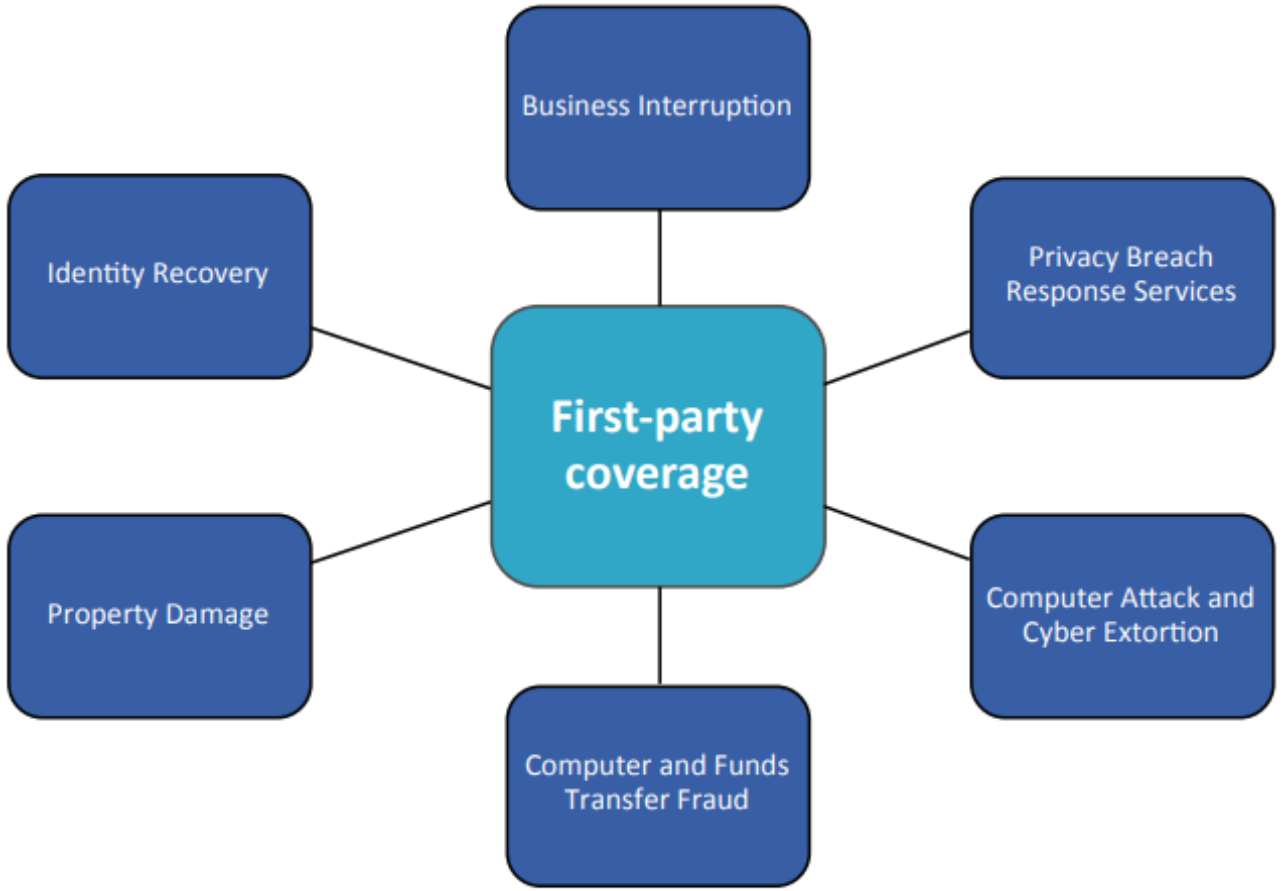
Business interruption loss often includes:

1. Income loss

(a.) Net profit (loss) before income taxes.
(b.) Fixed operating expenses including payroll incurred by the insured if:
• Expenses must necessarily continue during the period of restoration; and
• Expenses would have been incurred by the insured had such interruption or suspension not occurred.

2. Extra expense

(a.) Reasonable and necessary expenses incurred by the insured during the period of restoration to minimize, reduce or avoid income loss.
(b.) Forensic expense—Reasonable and necessary expenses incurred by the insured to investigate the source or cause of the failure of computer security to prevent a security breach.



Cyber Business Interruption Examples

UC RIVERSIDE Office of Emergency Management

Incident	Approximate Attack Date / Disclosure	Approximate Attribution Date	Alleged Attacker	Attributed By
Sands Casino[120121]	02/11/2014	09/10/2015	Iran	United States
Sony Pictures Entertainment[122]	11/24/2014	12/19/2014	North Korea	United States
Office of Personnel Management Breach[123124]	06/05/2015	09/21/2018	China	United States
Wannacry[125]	05/12/2017	12/19/2017	North Korea	United States, United Kingdom, Australia, Canada, New Zealand, and Japan
Equifax Breach[126]	05/13/2017	02/10/2020	Chinese PLA	United States
NotPetya[127,128]	06/27/2017	02/14/2018	Russian military	United States,
United Kingdom, etc.				
Russian Cyber-Attack on Georgia[129,130]	10/28/2019	02/27/2020	Russian GRU	United States,
United Kingdom, etc.				
Solar Winds' Orion[131,132]	12/14/2020	01/05/2021	Russia SVR	United States
Microsoft Exchange Server Attack[133,134]	03/02/2021	07/19/2021	Chinese MSS	United States, United Kingdom, EU, NATO
Colonial Pipeline Attack[135,136]	05/07/2021	05/10/2021	DarkSide	United States
JBS Attack[137,138]	05/31/2021	06/02/2021	REvil (aka Sodinokibi)	United States
Kaseya Attack[139]	07/02/2021	07/04/2021	REvil	Self-acknowledged by REvil

‘NotPetya’ Cyber Insurance Litigation

UC RIVERSIDE Office of Emergency Management

Mondelez v. Zurich

On June 27, 2017, one of the major global cyberattacks, NotPetya, commenced and Ukrainian companies were among the first victims. The NotPetya malware resembled the original Petya virus but spread easily and quickly infected internet networks and disabled computers. Despite a demand for a ransom to unlock these computers, the attack is believed to have been designed to cause massive destruction rather than extortion. Cybersecurity experts believe the attacks were designed to spread as quickly as possible. Shortly after, companies in several other countries including major corporations such as Mondelez International, FedEx, and Maersk among many others were infected. Under a cyber insurance policy, the NotPetya attack would likely trigger a property damage and/or computer attack and cyber extortion coverage from a first party’s perspective. This would potentially cover physical loss or damage to electronic data, programs, or software. However, some insurers have defined this cyberattack as an “act of war,” an insurance coverage specifically excluded in the policy definition.

Zurich Insurance has denied Mondelez’s claim for losses suffered in the 2017 NotPetya attack due to Zurich’s “hostile or warlike action” clause and at time of publication this is under litigation in Illinois state court. The policy was a property policy.

Cyber Insurance Timeline

UC RIVERSIDE Office of Emergency Management

MARSH COMMERCIAL

History of cyber insurance