OEM:
Weekly SITREP

April 12, 2022
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.

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.

- Paradise: a group which targets utilities, aerospace and oil and gas companies in Europe and the Middle East. This group uses open-source tools and known vulnerabilities for initial access. Paradise is suspected to be linked to Iran.
- Xenel: a group which targets oil & gas companies in the United States and Australia. It’s believed the group is linked to Russia.
- Magnallium: a group which initially targeted oil and gas companies in Saudi Arabia, which has expanded to target Europe and North America. It’s thought to be related to APT 33, a state-sponsored actor hacking group.
- Dynamic: a group which targets electric utilities, oil and gas and other critical industrial entities across Europe, Turkey and North America. Described as “highly aggressive”, Dynamic 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 the crash overridden – also known as Indiostorm – a malware attack on Ukraine’s power grid in December 2019. Electrum is associated with Sandworm, an offensive hacking operation that’s part of Russia’s GRU military intelligence agency.
- Allentale: a group which targets enterprise and OT networks in the UK and US, electricity sectors, as well as German industrial infrastructure and uses access to conduct reconnaissance on networks to potentially stage future disruptive events. It’s believed Allentale is linked to Russia.
- Chryser: active since at least 2017, this group has targeted industrial organisations in Europe and the Middle East, as well as other industries, conducting intelligence-gathering operations to potentially facilitate further attacks. Chryser is suspected to be linked to Iran.
- Kamad: 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.
- Cove: a group which has targeted electric utilities in the US, and East Asia, using malicious attachments to phishing emails. The group is believed to be linked to the Lazarus Group, a state-backed hacking group working out of North Korea.
- Varranalde: a hacking group which targets global firms in the oil and gas sector. It is 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.
**The County of Riverside Emergency Operations Center is currently activated to Management Watch.**

- 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.
• 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

- 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.
Global Business Risk 2022

- Cyber incidents: 44%
- Business interruption: 42%
- Natural catastrophes: 25%
- Pandemic outbreak: 22%
- Changes in legislation and regulation: 19%
- Climate change: 17%
- Fire, explosion: 17%
- Market developments: 15%
- Shortage of skilled workforce: 13%
- Macroeconomic developments: 11%
Systemic Cyber Risk & Interdependency

- 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

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

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

<table>
<thead>
<tr>
<th>Incident</th>
<th>Approximate Attack Date / Disclosure</th>
<th>Approximate Attribution Date</th>
<th>Alleged Attacker</th>
<th>Attributed By</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sands Casino</td>
<td>02/11/2014</td>
<td>09/10/2015</td>
<td>Iran</td>
<td>United States</td>
</tr>
<tr>
<td>Sony Pictures Entertainment</td>
<td>11/24/2014</td>
<td>12/19/2014</td>
<td>North Korea</td>
<td>United States</td>
</tr>
<tr>
<td>Office of Personnel Management Breach</td>
<td>06/05/2015</td>
<td>09/21/2018</td>
<td>China</td>
<td>United States</td>
</tr>
<tr>
<td>Wannacry</td>
<td>05/12/2017</td>
<td>12/19/2017</td>
<td>North Korea</td>
<td>United States, United Kingdom, Australia, Canada, New Zealand, and Japan</td>
</tr>
<tr>
<td>Equifax Breach</td>
<td>05/13/2017</td>
<td>02/10/2020</td>
<td>Chinese PLA</td>
<td>United States</td>
</tr>
<tr>
<td>NotPetya</td>
<td>06/27/2017</td>
<td>02/14/2018</td>
<td>Russian military</td>
<td>United States,</td>
</tr>
<tr>
<td>Russian Cyber-Attack on Georgia</td>
<td>10/28/2019</td>
<td>02/27/2020</td>
<td>Russian GRU</td>
<td>United States,</td>
</tr>
<tr>
<td>United Kingdom, etc.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Solar Winds’ Orion</td>
<td>12/14/2020</td>
<td>01/05/2021</td>
<td>Russia SVR</td>
<td>United States</td>
</tr>
<tr>
<td>Microsoft Exchange Server Attack</td>
<td>03/02/2021</td>
<td>07/19/2021</td>
<td>Chinese MSS</td>
<td>United States, United Kingdom, EU, NATO</td>
</tr>
<tr>
<td>Colonial Pipeline Attack</td>
<td>05/07/2021</td>
<td>05/10/2021</td>
<td>DarkSide</td>
<td>United States</td>
</tr>
<tr>
<td>JBS Attack</td>
<td>05/31/2021</td>
<td>06/02/2021</td>
<td>REvil (aka Sodinokibi)</td>
<td>United States</td>
</tr>
<tr>
<td>Kasoya Attack</td>
<td>07/02/2021</td>
<td>07/04/2021</td>
<td>REvil</td>
<td>Self-acknowledged by REvil</td>
</tr>
</tbody>
</table>
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

**History of cyber insurance**

- **1990s**
  - Initially cyber insurance covers were add-ons to existing liability covers for companies operating in the technology and professional services sectors.

- **2005**
  - Some of the first cyber products only covered 3rd party liabilities, like issues affecting a business’s clients, however by the mid-2000s some 1st party covers such as - losses to the businesses themselves, were being provided.

- **2010**
  - The increase in demand for cyber insurance products coincided with the growing cyber risks faced by businesses leading to cyber liability insurance being increasingly sold as a standalone product.

- **2016**
  - A string of high profile data breaches and the associated costs illustrated the need for cyber insurance regardless of the industry a business operates within. This drove greater demand for cyber insurance products.

- **2018**
  - General Data Protection Regulation (GDPR) came into force, raising the profile of cyber risks for all businesses.

- **2020**
  - COVID-19 forced most organisations to work remotely, resulting in an unprecedented increase in the use of mobile devices and remote access to core business systems. Cyber criminals have seen the pandemic as an opportunity to exploit unsecure devices. Raising awareness once more of the need for appropriate cyber insurance.

- **2021**
  - “Silent cyber” cyber and the insurers’ stance on this, has brought cyber insurance into focus once more. Silent cyber refers to potential cyber exposures contained within traditional property and liability insurance policies which may not implicitly include or exclude cyber risk. It is sometimes also called “non-affirmative” cyber.\(^1\)