Cyber Insurance

Are cyber-attacks insurable?
Insurance insight, guidance and relevance

Mark Luckin, Cyber & Technology Practice Leader

LOCKTON®

What?

What's topical?

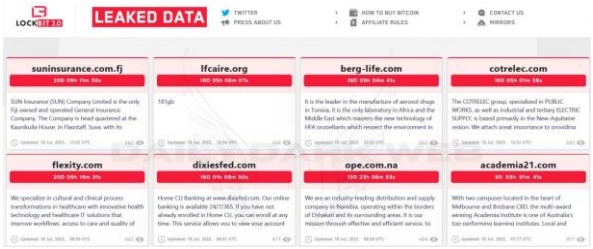
Can anyone think of some recent examples….?

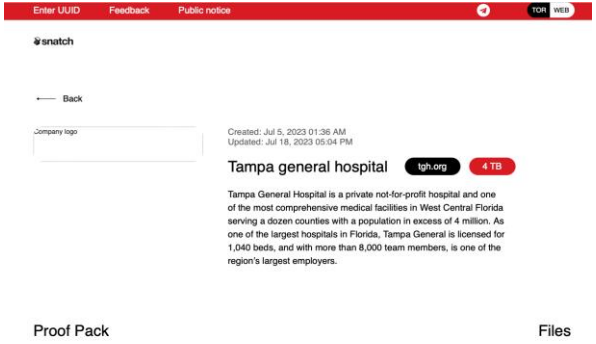
How?

INSIDE THREATS

OUTSIDE THREATS

Why?


LOCKBIT 3.0
LEAKED DATA
TWITTER
PRESS ABOUT US
HOW TO BUY BITCOIN
AFFILIATE RULES
CONTACT US
MIRRORS
suninsurance.com.fj
lfcaire.org
berg-life.com
cotrelec.com
flexity.com
dixiesfed.com
ope.com.na
academia21.com


Enter UUID
Feedback
Public notice
TOR
WEB
snatch
Back
Company logo
Created: Jul 5, 2023 01:36 AM
Updated: Jul 18, 2023 05:04 PM
Tampa general hospital
tgh.org
4 TB
Tampa General Hospital is a private not-for-profit hospital and one of the most comprehensive medical facilities in West Central Florida serving a dozen counties with a population in excess of 4 million. As one of the largest hospitals in Florida, Tampa General is licensed for 1,040 beds, and with more than 8,000 team members, is one of the region's largest employers.
Proof Pack
Files

Healthcare stats

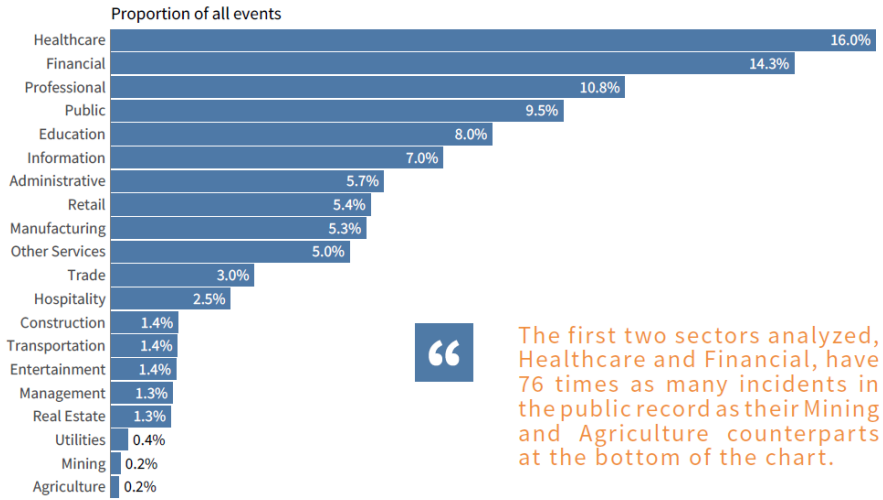


Figure 2: Proportion of publicly known incidents attributed to each sector

The first two sectors analyzed, Healthcare and Financial, have 76 times as many incidents in the public record as their Mining and Agriculture counterparts at the bottom of the chart.

Losses observerved per sector		
Sector	Geometric mean	95th percentile
Administrative	$183K	$50M
Agriculture	$61K	$3M
Construction	$66K	$6M
Education	$139K	$5M
Entertainment	$468K	$92M
Financial	$437K	$88M
Healthcare	$211K	$13M

Consequences

INCIDENT RESPONSE

Ransomware Attack Played Major Role in Shutdown of Illinois Hospital

St. Margaret's Health in Illinois is shutting down hospitals partly due to a 2021 ransomware attack that caused serious payment system disruptions.

By Ionut Arghire
June 13, 2023

St. Margaret's Health is shutting down hospitals and other facilities in Peru and Spring Valley, Illinois, and says a 2021 ransomware attack is partly to blame.

The attack occurred in late February 2021 and forced the shutdown of the Spring Valley hospital's computer network, impacting all web-based operations, including its patient portal. The Peru branch was not affected, as it operated on a separate system.

The incident, the hospital said on social media, impacted its ability to bill patients and get paid in a timely manner for the provided services. The systems were down for more than three months.

Compounded with impact from the Covid-19 pandemic, a shortage of staff, and rising costs of goods and services, the cyberattack forced the hospital to suspend some of its services in January this year.

TRENDING

1. Microsoft Warns of Office Zero-Day Attacks, No Patch Available
2. MOVEit Hack: Number of Impacted Organizations Exceeds 340
3. Hackers Target Reddit Alternative Lemmy via Zero-Day Vulnerability
4. JumpCloud Says Sophisticated Nation-State Hackers Targeted Specific Customers
5. Exploitation of Coldfusion Vulnerability Reported as Adobe Patches Another Critical Flaw
6. SecurityWeek Analysis: Over 210 Cybersecurity M&A Deals Announced in

What can you do?

INFORM

IMPROVE

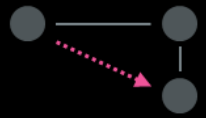
INSURE

What is Cyber Insurance?

FIRST-PARTY COVERAGES

Compensate insureds for their own losses resulting from covered cyber events. Claims may arise from breaches, suspected breaches, suspicious activity on networks and cyberattacks.

THIRD-PARTY COVERAGES



Pay others for insureds' liability to them for losses arising from covered cyber events and/or wrongful act. Claims can include written demands, regulatory inquiries, complaints and fines and penalties.

What role does Cyber Insurance play in a Cyber Attack?

Cyber policies typically cover the reasonable and necessary expenses to investigate and remediate an event an associated liabilities.

However the real value is…

24/7 - 365

Incident response

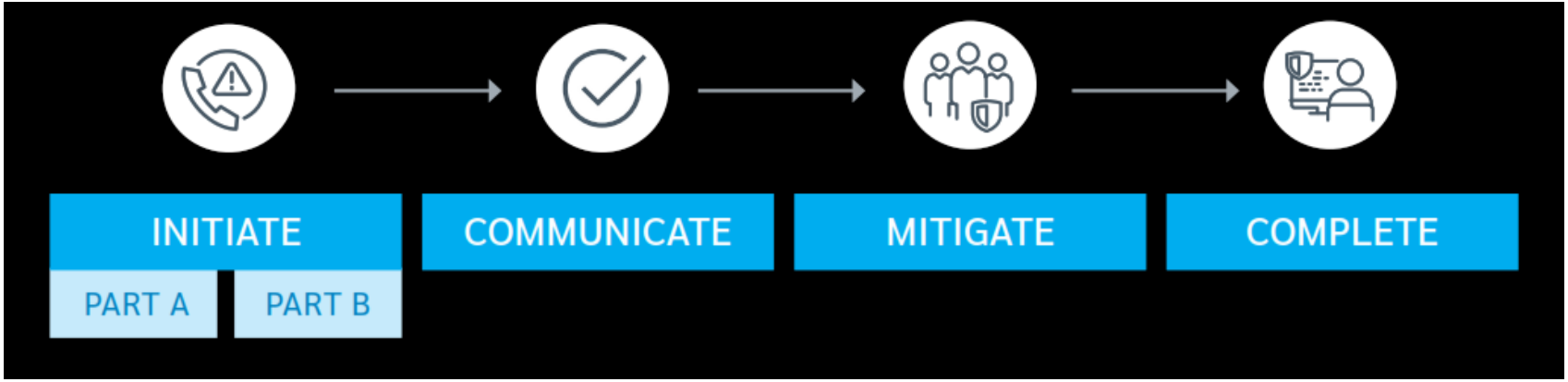
- Incident response strategy
- Legal and regulatory compliance
- Data review and privacy risk assessment
- Stakeholder management / crisis communications
- Vendor selection and engagement
- Insurance claims management (if applicable)
- Threat actor engagement / sanctions compliance
- Media and dark web monitoring

How does the Cyber Insurance claim process work?

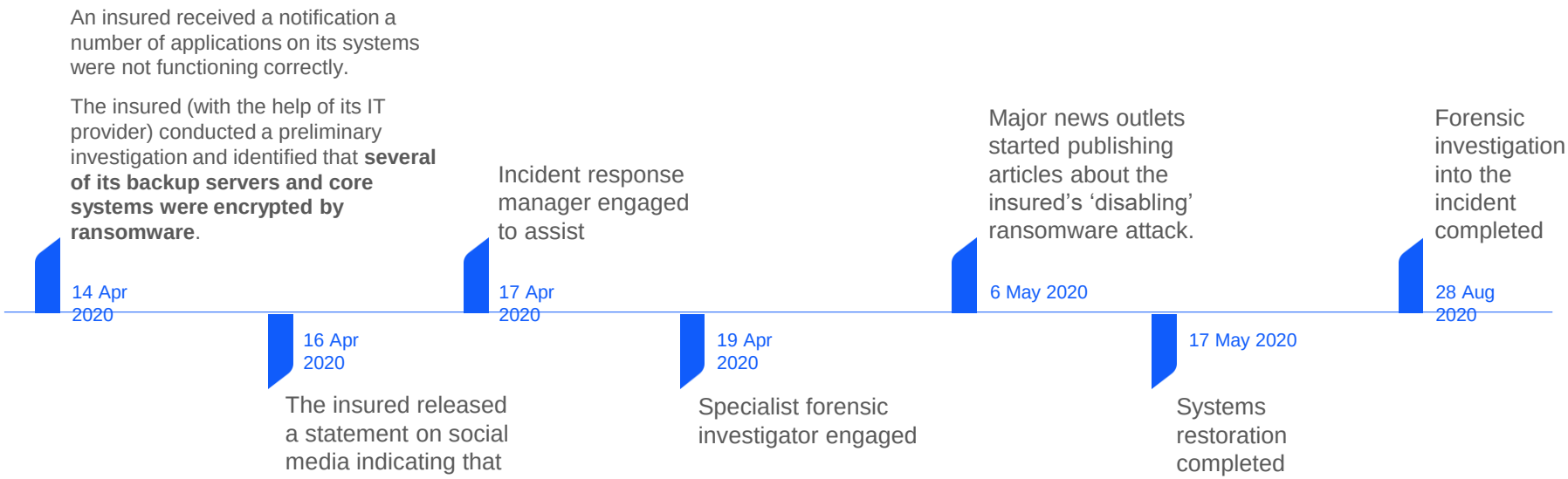
Each cyber insurance attack is unique and will have its own nuances.

Several factors — both internal and external — will determine how a claim proceeds and how long the process will take.

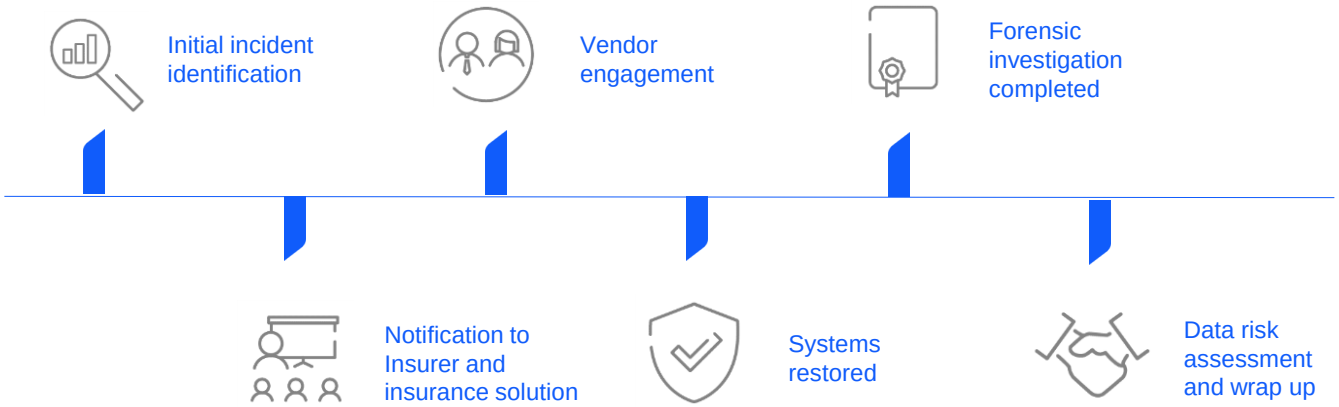
Outlined over the next few slides are the steps and best practices for organisations to consider when faced with a cyber insurance attack. The claim process will often run in parallel with an organisation's incident response process and be facilitated by an Incident Response Manager.



Incident case study 1 – Ransomware - What happened



Timeline of activities



Summary of costs involved

Component	Cost
1. Incident Response Coordination	$20,000
2. Privacy Assessment and Advice	$10,000
3. Communications and Stakeholder Management	$10,000
4. Containment and Remediation	$150,000
5. Forensic Investigation	$110,000
6. Staff Costs	$250,000
Total to date	**$550,000**

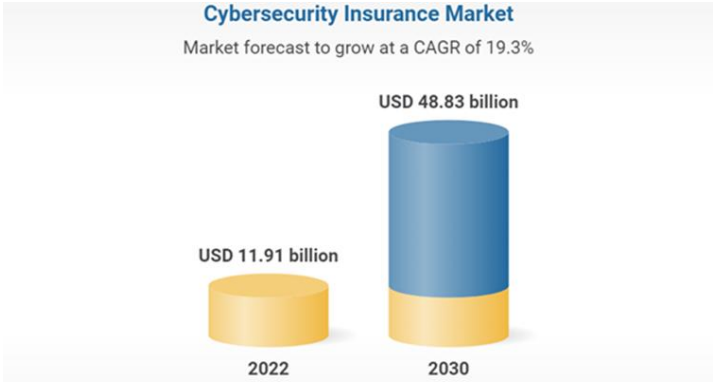
Cyber Insurance Market

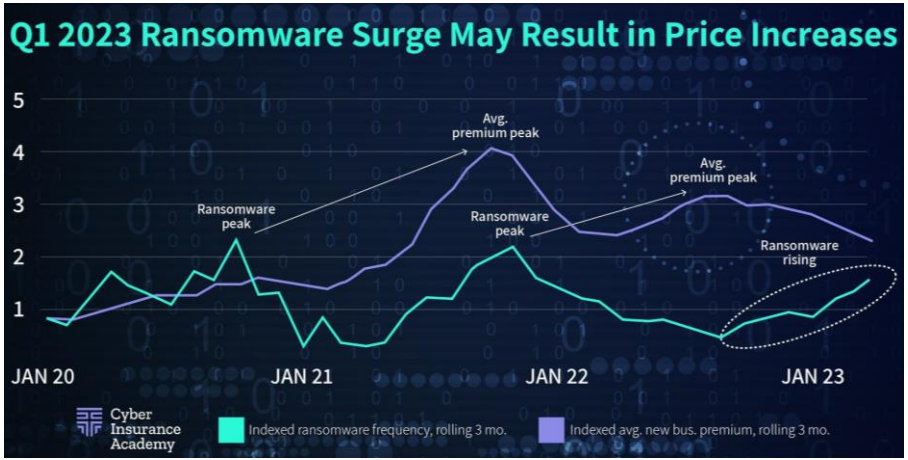
The Cybersecurity Insurance Market was estimated to be valued at $11.91 billion in 2022 and is expected to reach USD 48.83 billion by 2030.

Conditions in the cyber insurance market are far more favourable than they were just a quarter ago, with insurers increasingly competing for risks as they focus on growth.

Even as insurers increasingly compete for new business, they continue to scrutinise cybersecurity controls, and be conscious of re-emerging ransom threats and legislative changes with respect to data and privacy.

Insurers are focusing on limiting their exposure to large events that can produce significant losses to many insureds.





Questions