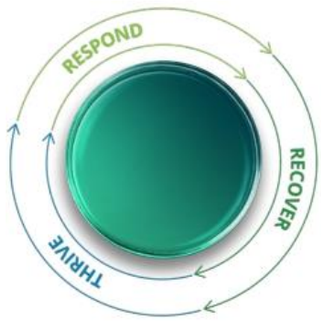
Deloitte.

德勤

Global Cyber COVID-19 weekly executive cyber briefing

A weekly high-level brief that focuses on some of the most current cyber threats and trends as identified by Deloitte Cyber Threat Intelligence (CTI), with near-term recommendations on managing cyber risks to respond, recover and thrive through the COVID-19 global pandemic.

Please note: *Page 1 focusses on healthcare critical infrastructure, page 2 includes industry agnostic thought leadership on cyber implications in critical infrastructure*



2 | April 2020

The cyber impacts amid COVID-19 on healthcare critical infrastructure

Our healthcare organizations are on the front lines combatting the COVID-19 pandemic when they find themselves ambushed by unscrupulous cyber attackers. As a result, these organizations are now fighting on two fronts during one the most challenging times in their history. Research from Deloitte Cyber Threat Intelligence (CTI) indicates COVID-19 (coronavirus) pandemic responses by healthcare providers and research institutes are hampered by cyber adversaries who are launching cyber-attacks around the globe targeted at critical health care infrastructure. **This week we highlight a few of the issues and related cyber threats** (and originally identified in our detailed threat report dated March 13 - April 10) impacting healthcare organizations globally.

Impact reach: Life Sciences and Healthcare / Geographies: Global

Attacks on computer systems prohibit COVID-19 test results

On March 13, 2020, computer systems at the University Hospital Brno in the Czech Republic were breached as a result of a cyber-attack. The Czech Republic hospital hosts one of the largest testing laboratories for coronavirus. All the hospital's computers were forced shut down as a result of this breach, leading to a delay in test results.

Suggested top actions:

1. Avoiding clicking on attachments/links embedded in email messages with subject lines purporting to contain information related to COVID-19 or Coronavirus.
2. Using firewalls and intrusion detection/prevention systems (IDS/IPS) to detect and block network communications with malware Command and Control (C2) nodes.
3. Consider alerting based on emails containing references to COVID-19, coronavirus, and other keywords which contain uncommon file types.

Breaches to national health systems disrupt continuity of services

On March 15, 2020, the U.S. Health and Human Services Department (HHS) fell victim to a cyber-attack. The attack was likely intended to disrupt operations and an attempt to undermine the response to the coronavirus pandemic and may have been the work of a foreign threat actor. The attack involved overloading the HHS servers with millions of hits over several hours (a.k.a. distributed denial of service attack - DDoS). Government officials also noticed false information regarding a national lockdown being circulated via text messages, email, and social media. The National Security Council (NSC) addressed this disinformation incident by warning via their Twitter account that such messages about a national lockdown are false.

Suggested top actions:

1. To mitigate DDoS attacks, identify/understand your organization's upstream service providers and collaborate with the providers to develop strategies for redundancy
2. Configure network devices to silently drop packets from blacklisted zones
3. Purchase DDoS mitigation service from dedicated providers and implement Border Gateway Protocol (BGP)-based DDoS scrubbing.

Ransomware impedes work at COVID-19 vaccine test centers

On March 23, 2020, an attack campaign targeted the healthcare provider Hammersmith Medicines Research, which is associated with the British Government to test the Coronavirus (COVID-19) vaccine. The British medical facility was hit by the Maze ransomware attack that stole the user data to demand a ransom. People familiar with the attack indicated that the ransomware attack occurred on March 14, 2020; however, it was contained until it after it was made public in the news on March 23, 2020. The threat actors managed to collect some of the patient data and posted it online in order to get payment for the ransom they demanded. Threat actors behind the maze ransomware announced on March 18, 2020, they would not target medical organizations during the Coronavirus pandemic. However, this pledge did not stop them from continuing to collect a ransom.

Suggested top actions:

1. Relying on strong, frequent, and redundant backups to recover files from a ransomware or destructive malware infection.
2. Identifying your most sensitive or mission-critical systems and data and provide them with extra levels of protection, such as network segmentation or encryption.
3. Mapping the attack surface of your public-facing infrastructure and identify ways to harden or shut down potential points of entry for attackers.

Top trends in Cyber impacts to health service providers and health research institutes during COVID-19 pandemic

- COVID-19 vaccine IP theft
- Supply chain compromise
- Ventilator and medical device compromise
- Malicious COVID-19 phishing campaigns
- Advanced persistent threats (APTs)
- Targeting of remote working/ telemedicine video conference platforms
- COVID-19 patient Electronic Health Record/Personal Health Information

Recommendations to stabilize capabilities

- Review and update cloud security strategies to support virtual health innovations
- Perform accelerated security reviews of third parties providing support services for COVID-19 response
- Extend threat detection and monitoring capabilities to remove devices

'Getting ahead' to normalize and scale

- Expand security architecture to incorporate additional business use cases for virtual health care delivery
- Implement user and entity behavior analytics (UEBA) for remote devices
- Establish or enhance a crisis preparedness program and conduct pilot runs

150%

Cyber attacks In two months

in the healthcare sector as criminals seek to take advantage of system vulnerabilities during the COVID-19 crisis.

Reference: https://www.medicaldevice-network.com/news/coronavirus-cybersecurity/)

Recover and Thrive: COVID-19 spurs the next normal of critical infrastructure

A number of global manufacturing and logistics organizations have been asked to take extended roles and are now included in what could be termed as "public welfare" organizations and as such part of a country's critical infrastructure. As an extension of this new alignment, the supply chains of these organizations are also now part of the country's critical infrastructure (for example, medical and other critical supplies produced and distributed for healthcare workers) – because without suppliers and logistics companies, these organizations cannot function. New designees also include research labs, supermarkets and other retailers selling necessities. The US Department of Homeland Security (DHS) added the for-hire transportation sector to its list of "essential critical infrastructure workers" amid the COVID-19 pandemic.

As part of the country's critical infrastructure, the organizations are now required to meet a variety of cybersecurity and privacy regulations. Previously, these organizations had minimal cybersecurity compliance requirements, and those were in the context of ISO quality standards, not government-mandated cybersecurity standards. But now, as part of the country's critical infrastructure, the organizations are required to meet a variety of cybersecurity and privacy regulations.

COVID-19 Impact – Manufacturing and logistics organizations | From Non-Essential to Critical, Overnight

A number of manufacturing and logistics organizations have been asked to take extended roles and have been included in what could be termed as "Public Welfare" organizations and as such part of a country's critical infrastructure, due to the COVID-19 outbreak, it had been reclassified as "critical" since products and services are required for public welfare (as part of medical and other critical supplies production and distribution for healthcare workers, for example). Previously, these organizations had minimal cybersecurity compliance requirements, of which were in the context of ISO quality standards, not local government-mandated cybersecurity standards. But now, as part of it's critical infrastructure, companies now must meet a variety of cybersecurity and privacy regulations. This will require extensive re-architecting of manufacturing and logistics organizations' security infrastructure, so it can meet government standards and alleviate the cost, time and effort of compliance reporting in order to avoid non-compliance resulting in potential fines.

The Next Normal

Organizations that now find themselves a part of critical or vital infrastructure industries will need to expand or reallocate budgets to fund necessary digital transformation initiatives and regulatory compliance actions that focus on business resiliency and employee enablement, along with the customer engagement and revenue generation initiatives that pre-date the pandemic.

Government agencies around the globe have associations to provide guidance on regulatory shifts related to critical infrastructure services and detail how a risk management framework and approach to critical infrastructure security should be implemented for a particular industry sector.

Coordination with such groups will enable newly labeled organizations to not only survive the next major disruption; but thrive at an accelerated level, during times of crisis, to deliver the essential products and services stakeholders need. This may inform the definition of success in the next normal of critical infrastructure.

Being compliant does not equal mature security capability

Organizations should consider the following to ensure measurable security infrastructure controls are in place across critical applications and core infrastructure.

- **A secure operating environment should include:** patching currency and vulnerability assessment of material infrastructure and applications
- **Institute cyber incident response** monitoring and reporting. Update playbooks and business continuity and disaster recovery plans
- **Discovery and security of critical data assets** as required under Personally Identifiable Information obligations for citizen and staff data
- **Identify and secure third-party suppliers** who had approved direct access to the organization's systems and then gain a further understanding of any fourth or fifth parties required via the third party

We're by your side to help you through COVID-19

Relevant Deloitte reads:

- **On-Demand Webcast:** **Responding to COVID-19 with business resilience, trust, and security**
- **Article:** **Ransoming government**
- **Article:** **COVID-19 response capabilities for health care organizations**
- **Article:** **The heart of resilient leadership: Responding to COVID-19**

Deloitte Cyber helps organizations perform better, solving complex problems so they can build confident futures. Smarter, faster, more connected futures—for business, for people, and for the planet. As a recognized leader in cybersecurity consulting, Deloitte Cyber can help better align cyber risk strategy and investments with strategic business priorities, improve threat awareness and visibility, and strengthen our clients' ability to thrive in the face of cyber incidents. Deloitte Cyber uses human insight, technological innovation and comprehensive cyber solutions, to manage cyber everywhere, so society can go anywhere.

Deloitte China Cyber Risk Partners


Xue, Tonny
National Cyber Risk Leader
Tel: +86 10 8520 7315
E-mail: tonxue@deloitte.com.cn


Jiang, David Wei
Eastern Region
Tel: +86 21 2312 7088
E-mail: davidjiang@deloitte.com.cn


He, Tommy Xiaoming
Northern Region
Tel: +86 10 8512 5312
E-mail: the@deloitte.com.cn


Kwok, Eva Yee Ngar
Southern Region, Hong Kong
Tel: +852 2852 6304
E-mail: evakwok@deloitte.com.hk


Feng, Steven Ye
Eastern Region
Tel: +86 21 6141 1575
E-mail: stefeng@deloitte.com.cn


Shih, Nathan Pei-en
Eastern Region
Tel: +86 21 3313 8366
E-mail: nathanshih@deloitte.com.cn


Xiao, Frank Tengfei
Northern Region
Tel: +86 10 8512 5858
E-mail: frankxiao@deloitte.com.cn


Pihkanen, Miro
Southern Region, Hong Kong
Tel: +852 2852 6778
E-mail: miropihkanen@deloitte.com.hk


Kukreja, Puneet
Eastern Region
Tel: +86 21 3313 8338
E-mail: puneetkukreja@deloitte.com.cn


Zhang, Boris Zhen
Eastern Region
Tel: +86 21 6141 1505
E-mail: zhzhang@deloitte.com.cn


He, Vivi Wei
Southern Region
Tel: +86 755 3353 8697
E-mail: vhe@deloitte.com.cn


Ma, Luke Kwok Kwan
Southern Region, Hong Kong
Tel: +852 2852 1086
E-mail: lukema@deloitte.com.hk

For more information contact visit Deloitte.com/covid or Deloitte.com/cyber