

IN THE CROSSHAIRS OF CYBERCRIMINALS –

# Houston's Infrastructure Industries Are Under Attack

**O**n December 25, 2009, I<sup>1</sup> moved from Kentucky to Washington, D.C. to join the Department of Justice's Counterterrorism Section and its Al Qaeda Unit, joining an international effort to bring Al Qaeda's terrorists to justice. At the time, U.S. intelligence agencies considered Al Qaeda the country's primary national security threat.<sup>2</sup> In fact, on that Christmas morning more than 15 years ago, while I drove into Washington for the first time, a Nigerian national, Umar Farouk Abdulmutallab, arrived in Detroit attempting to ignite a bomb hidden in his underwear on behalf of Al Qaeda in the Arabian Peninsula—an Al Qaeda affiliate based in Yemen.<sup>3</sup> Although passengers subdued Abdulmutallab before he could cause any harm, he brought home the notion that Al Qaeda was still a threat to the homeland more than eight years after the September 11, 2001 attacks.

Much has changed since then. According to the U.S. intelligence community, the People's Republic of China ("China") has eclipsed Al Qaeda as the largest national security threat, and instead of attacking us with bombs, planes, or martyrs, China, Russia, North Korea, and criminal organizations—often working with nation-states—deploy weapons that don't target physical structures, but rather the nation's

cyber network.<sup>4</sup> And they are primarily targeting America's businesses with a focus on America's critical infrastructure.

According to the Cybersecurity and Infrastructure Security Agency ("CISA"), a U.S. federal agency responsible for safeguarding national cybersecurity and protecting critical infrastructure against threats, "[t]here are 16 critical infrastructure sectors . . . so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."<sup>5</sup> Cybersecurity in these industries is crucial since any disruption or breach can lead to significant impacts on public safety, the economy, and national security. Four critical infrastructure sectors call Houston home—energy, health care, transportation (including the Port of Houston and two major airports), and a large concentration of chemical manufacturing companies. It is why Houston's businesses and public utilities are on the front lines of America's war against cyberattacks from government actors and criminal organizations.

Cybercriminals use a variety of tools—phishing, malware, ransomware (a type of malware), and insider threats—to steal information and to generally cause havoc. Ransomware is a particularly powerful tool, allowing a cybercriminal to encrypt a victim's files, then demand a ransom for the decryption key. Ransomware can paralyze systems, disrupt operations, and inflict financial loss. Ransomware has become so effective that it is now an underground industry, offered as a service called Ransomware as a Service (RaaS).<sup>6</sup> Through this business model, ransomware developers offer their ransomware code to affiliates (for a fee), which allows the affiliates to launch their own ransomware attacks. The RaaS business model enables developers to increase their profits beyond running attacks themselves.

A stark example of a ransomware attack on a key infrastructure industry occurred early in 2024, when a hacking group with ties to Russia known as BlackCat or ALPHAV instituted a hack that crippled a portion of the health care system and exposed the data of 190 million Americans—or

CYBER  
ATTACK DETECTED

DETAIL



more than half the U.S. population.<sup>7</sup>

Change Healthcare, owned by UnitedHealth Group, manages health care technology pipelines and “acts as a clearing house for 15 billion medical claims each year—accounting for nearly 40 percent of all claims.”<sup>8</sup> In February 2024, BlackCat used stolen credentials to gain initial access to Change Healthcare’s network. These credentials provided access to a server that did not have multifactor authentication enabled; a security process that requires users to verify their identity through multiple methods—such as a password, a fingerprint, or a verification code—before gaining access to a system or account. Once inside, the attackers moved within the network, exploring and gaining access to various systems and data. BlackCat then exfiltrated a vast amount of sensitive data undetected before deploying the ransomware.<sup>9</sup> The ransomware encrypted files and disabled large portions of Change Healthcare’s operations, causing widespread chaos for weeks, which included critical functions such as claims processing, prescription management, payment, prior authorization, and insurance verification. Hospitals reported delays in authorizations and disbursements causing financial strains. According to a survey by the American Hospital Association, “[n]early all hospitals (94%) said they have suffered a financial impact from the Change Healthcare attack [and] [n]early 60% of the hospitals said the impact on their revenue has been \$1 million per day or greater.”<sup>10</sup> Eventually, Change Healthcare paid a \$22 million ransom to obtain a decryption key and prevent the publication of stolen data. Despite the payment, the cybercriminals retained the stolen data, and the attack had lasting implications for the health care industry.<sup>11</sup>

### Attacks on Third-Party Vendors

Besides attacks directly to a company’s systems, vendors are also a vector of attack. For example, in December 2020, hackers associated with the Russian government infiltrated the systems of SolarWinds, an IT management company, and planted malware giving them backdoor access to the networks of SolarWinds’ clients. Many of SolarWinds’ clients were U.S. government

agencies, and by compromising SolarWinds, the attackers were able to move laterally into the systems of more than 18,000 organizations, including key federal agencies, such as the Department of Homeland Security, the State Department, and the Departments of Commerce and the Treasury. The attack highlighted the vulnerabilities in software supply chains, chains outside of a company’s internal cyber infrastructure; vulnerabilities exploited by both cyber criminal enterprise and hostile nation-state actors.<sup>12</sup>

### Nation-State Sponsored Attacks

Nation-state actors possess advanced tools and capabilities developed or acquired through significant investment in research and development. Like cyber criminal enterprises, they deploy a range of tactics, from phishing and malware to sophisticated exploitation of software vulnerabilities. But unlike the cyber criminal enterprises, their actions are not just aimed at financial gain but are part of a broader strategy to disrupt, destabilize, and gather intelligence. A key

feature of state-sponsored groups is the patience to plan for the long-term. The most sophisticated nation-state actor is China.

### China-Sponsored Attacks

China’s goal is to assert geopolitical leverage so it can surpass the U.S. as the world’s leading global superpower, and by targeting critical infrastructure, China seeks to gather intelligence, exploit vulnerabilities, and potentially disrupt operations in times of conflict or heightened tension. In essence, when the time is right, “wreak havoc and cause real-world harm to American citizens and communities.”<sup>13</sup>

That came to light with a group associated with China’s military, Volt Typhoon. Discovered in 2023, the Volt Typhoon hackers employed advanced stealth techniques to infiltrate various organizations. They infected old Small Office/Home Office (SOHO) routers, due to weak passwords, outdated firmware, or unpatched software. By controlling SOHO routers, Volt Typhoon established a covert command and control infrastructure that deployed malware

**LIFT OFF HAS OCCURRED, CARLA COTROPIA IS NOW**

# COTROPIA MEDIATIONS PLLC



**SETTLING CASES TWO SNEAKERS AT A TIME**

**Carla's new contact info: 832-615-2920**

**cc@cotropiamediations.com**

**SUSANNE (ASSISTANT): st@cotropiamediations.com**

**WEBSITE: cotropiamediations.com**

**Booking online available**

within a targeted network without arousing suspicion, since traffic to and from these devices appeared legitimate.<sup>14</sup> Volt Typhoon then used the SOHO router cover to surreptitiously gain access into critical infrastructure systems ready to likely, as former FBI Director Wray testified, “wreak havoc.”<sup>15</sup>

While the Volt Typhoon campaign was in full swing, another China state-sponsored hack, the Salt Typhoon espionage campaign, was also underway. This hacking campaign began as early as 2022 and infiltrated the U.S. telecommunications infrastructure, compromising the systems of at least nine major providers, including AT&T and Verizon. This sophisticated attack, deemed the “worst telecom hack in U.S. history” by Senate Intelligence Committee Chairman Mark Warner, exploited vulnerabilities in outdated network devices, such as Cisco routers, to gain persistent access, harvest metadata, intercept unencrypted communications, and even targeted phones used by high-value government individuals, including President Donald Trump and Vice President J.D. Vance during the recent presidential campaign.<sup>16</sup>

### Impacts of Cyber Incidents

Unfortunately, the Change Healthcare, SolarWinds, and Volt Typhoon hacks are examples of hacks that occur every day on critical infrastructure industries, including Houston’s—attacks that have the potential to cost businesses millions. Houston’s companies must prepare for the inevitable cyber attack. According to IBM’s “Cost of a Data Breach Report 2024”, the average cost of a data breach rose in 2024 to \$4.88 million from \$4.45 million in 2023, due to both direct and indirect costs of responding to a breach.<sup>17</sup> Direct costs include operational downtime and the associated financial losses, as well as the costs to address the cyber incident itself, such as ransomware payments, regulatory fines, call center costs, or consumer protection measures. Indirect costs may include loss of customers, loss of reputation, or increased insurance premiums. For incidents involving critical infrastructure, the incident could result in public and environmental safety risks, such as threats to human life due to disruptions to essential services. These risks make critical

infrastructure a continued focus for regulation and a target for threat actors.

### Preparation Strategies

Cybersecurity is not the sole responsibility of your IT group but is an organization-wide effort. A first step in developing a good cybersecurity defense is building into your organization cybersecurity best practices. Best practices may differ depending on the size and nature of your organization, but there are several organizations that provide frameworks for cybersecurity: NIST Cybersecurity Framework,<sup>18</sup> North American Electric Reliability Corporation (“NERC”) Critical Infrastructure Protection,<sup>19</sup> ISO 27001, and ISO 27032.<sup>20</sup>

Generally, best practices include technical security measures, training, periodic audits and assessments, and recommended policies and procedures to implement, maintain, and improve cybersecurity programs. Technical security measures include access controls, encryption, and software updates that may be solely in the purview of an entity’s IT team. Training should include appropriate risk identification training for employees at every level of an organization. Audits and assessments can include both internal and external assessments and may include penetration testing or gap assessments.

### Responding to Cyber Incidents

One procedure that is critical for preparing for a cyber incident is an incident response plan—a guide for responding in the event of a cyber incident. A cyber incident response plan can borrow from other emergency response plans depending on the industry. A key component is identifying the internal team that will assemble in the event of an incident. NIST guidance includes steps for communications with outside parties, including external team members, preparation, detection and analysis, containment, eradication and recovery, and post-incident activity.<sup>21</sup> A great way to prepare for a cyber incident is to perform tabletop exercises, which gather the internal team in simulated events, and can test the effectiveness of different aspects of your plan.

The size and nature of your internal team will depend on your organization, but may include representatives from IT, legal, fi-

nance, human resources, public relations, outside counsel, and forensic experts. External communications may include notifications to insurance providers, law enforcement, regulators, and affected individuals (e.g., consumers or customers).

Insurance policies that cover cyber security risks, or cyber insurance, can be a key component of a cyber risk management strategy. But like all aspects of cyber risk management, it is critical that an organization understand the components of a cyber insurance policy. First, you and your broker must identify the types of events that should be covered. Understanding whether your industry is susceptible to ransomware attacks, cyber extortion events, or privacy claims can help tailor a policy to your business. Beyond the policy amounts, it is important to understand the requirements for invoking coverage. Effective cyber claims often require following a specific set of procedures, including making proper notifications and maintaining proper documentation. Advantageously, cyber insurance policies often provide access to experts that can assist in the event of an attack. One such expert is a ransomware negotiator.

As threat actors become more sophisticated, the response to their attacks has become correspondingly specialized. One role that has been crucial for responding to threat actors has been the ransomware negotiator. Much like a hostage negotiator, ransomware negotiators engage directly with the threat actor to negotiate the terms of settlement. Ransomware negotiators possess specialized knowledge of the threat actor landscape, often having detailed knowledge of individual attackers. They possess the technical skills to analyze the impact of an attack and can provide tools to assess the potential damage and aid with recovery. And they provide expertise on “industry” trends enabling you to get context for the scope of your payment.

Law enforcement can also be an important partner in identifying a threat actor. The FBI strongly encourages voluntary reporting to its Internet Crime Complaint Center at [ic3.gov](https://www.ic3.gov). Notification can unlock investigative resources, decryption tools, and coordination with entities like the U.S. Secret Service or Interpol, potentially miti-



gating damage or recovering assets. This can be especially important because paying ransoms—which is not illegal under U.S. law unless funding sanctioned groups—doesn't guarantee data recovery and may invite further attacks. Also, law enforcement can use its many tools to identify the bad actors, bank accounts, bitcoin wallets, and decryption keys. A key ingredient to law enforcement's success is speed, so the sooner a victim notifies law enforcement, the better.


Law enforcement uses many investigative tools to recover monies, identify perpetrators, and launch cyber tools to counteract attacks. These tools include grand jury subpoenas to banks and telecommunication companies, secured communications with foreign law enforcement partners, and sealed search warrants that remove malware. This work is done in secret and under seal. Despite that, companies fear reporting to law enforcement could lead to public exposure or regulatory scrutiny, so companies often weigh reporting against operational secrecy. Best practice leans toward notifying law enforcement for support and to bolster broader cyber defense, but it's a judgment call unless specific breach thresholds or sector rules require notification.

## Regulatory Notification

Timing and extent of notification to regulators depends on applicability of any rule and nature of the data compromised. Every state has a breach notification law requiring notification to consumers in the event personal data is compromised and many of these also require notification to the state attorney general. Many agencies, including the Securities and Exchange Commission, the NERC, the Department of Energy, Department of Defense, Department of Health and Human Services, and the Transportation Safety Administration (maintains pipeline security), and CISA, require notification or disclosures in the event of a cyber incident. Also, many foreign regulators require notifications that may conflict with or contradict the notifications required by the U.S. agencies, making it imperative that multi-nationals understand their global reporting regime. In essence, the regulatory notification scheme is complicated, making

it important to have a plan in place post-breach with the assistance of experienced legal counsel.

## Conclusion

On a snowy Christmas Day, just over 15 years ago, I began my career as a national security prosecutor. It started with me chasing Al Qaeda terrorists hiding in camps nestled in the mountains and hills of Afghanistan and Yemen and ended in Houston as the U.S. Attorney, where I led a cadre of prosecutors and investigators dedicated to disrupting hackers hiding behind encryption keys and keyboards in China and Eastern Europe. Over that time, I had to adapt as the threats became more complex, the attacks more constant, and the attackers more sophisticated. Although today's hackers are spread throughout the globe, their focus remains on Houston, targeting the businesses that serve the nation's critical infrastructure needs while caring little for the safety of the citizens that rely upon those key industries. 



**Alamdar Hamdani** is a litigation partner at *Bracewell, LLP* concentrating on government enforcement, white collar criminal defense, cybersecurity, and commercial litigation. Prior to joining *Bracewell*, Alamdar served in the Department of Justice, most recently as the United States Attorney for the Southern District of Texas.



**Lucy Porter**, a counsel in *Bracewell's* Houston office, advises clients on matters related to protecting their technology and information assets. She works with clients to develop and implement bespoke data privacy solutions that are compliant with global regulations, and she has experience working across organizations, including compliance, HR, security, IT, and legal.

## Endnotes

1. The first-person accounts throughout this article are from Alamdar. I appreciate my co-author allowing me the opportunity to share my story.
2. Annual Threat Assessment of the U.S. Intelligence Community for the Senate Select Committee on Intel-

ligence, 111th Cong. (2010) (statement of Dennis C. Blair), [https://isis-online.org/uploads/conferences/documents/2010\\_NIE.pdf](https://isis-online.org/uploads/conferences/documents/2010_NIE.pdf).

3. BBC, *Underwear Bomber Abdulmutallab Sentenced to Life*, Feb. 15, 2012, <https://www.bbc.com/news/world-us-canada-17065130>.
4. Annual Threat Assessment of the U.S. Intelligence Committee, Office of the Dir. of Nat'l Intelligence, Feb. 5, 2004, <https://www.dni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>.
5. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *Critical Infrastructure Sectors* <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors> (last visited Mar. 18, 2025).
6. CROWDSTRIKE, *Ransomware as a Service (RAAS) Explained How It Works & Examples*, <https://www.crowdstrike.com/en-us/cybersecurity-101/ransomware/ransomware-as-a-service-raas/> (last visited Mar. 18, 2025).
7. HEALTHCARE INNOVATION, *Change Healthcare Tallies 190 Million Data Breach Victims*, Jan. 27, 2025, <https://www.hcinnovationgroup.com/cybersecurity/data-breaches/news/55263828/change-healthcare-tallies-190-million-data-breach-victims> (last visited Mar. 18, 2025).
8. ENERGY & COMMERCE COMM., *What We Learned: Change Healthcare Cyber Attack*, May 3, 2024, <https://energycommerce.house.gov/posts/what-we-learned-change-healthcare-cyber-attack> (last visited Mar. 18, 2025).
9. *Examining the Change Healthcare Cyberattack: Hearing Before the House Committee on Energy & Commerce*, 118th Cong. (2024) (statement of Andrew Witty).
10. MEDICAL ECONOMICS, *Change Healthcare Breach Affected 100,000,000 Patients*, Oct. 28, 2024, <https://www.medicaleconomics.com/view/change-healthcare-breach-affected-100-000-000-patients> (last visited Mar. 18, 2025).
11. SECURITY INTELLIGENCE, *Change Healthcare Discloses \$22M Ransomware Payment*, May 24, 2024, <https://securityintelligence.com/news/change-healthcare-22-million-ransomware-payment/> (last visited Mar. 18, 2025).
12. TECHTARGET, *SolarWinds Hack Explained: Everything You Need to Know*, Nov. 3, 2023, <https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know> (last visited Mar. 18, 2025).
13. *Hearing Before the House Select Committee on Strategic Competition between the United States and the Chinese Communist Party*, 118th Cong. (2024) (statement of Christopher Wray).
14. Press Release, U.S. Dept. of Justice, U.S. Government Disrupts Botnet People's Republic of China Used to Conceal Hacking of Critical Infrastructure (Jan. 31, 2024), <https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical>.
15. See, *supra*, note 13.
16. Ellen Nakashima, *Top Senator Calls Salt Typhoon 'Worst Telecom Hack in Our Nation's History'*, Wash. Post, Nov. 21, 2024, <https://www.washingtonpost.com/national-security/2024/11/21/salt-typhoon-china-hack-telecom/>.
17. IBM, *Cost of a Data Breach Report 2024*, <https://www.ibm.com/reports/data-breach> (last visited Mar. 18, 2025).
18. NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, *Cybersecurity Framework*, <https://www.nist.gov/cyberframework> (last visited Mar. 18, 2025).
19. NERC, *Standards*, <https://www.nerc.com/pa/Stand/Pages/Default.aspx> (last visited Mar. 18, 2025).
20. INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *Information security, cybersecurity and privacy protection—Information security management systems—Requirements (ISO 27001:2022)*; INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *Cybersecurity—Guidelines for Internet Security (ISO 27032:2023)*.
21. NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, *Computer Security Incident Handling Guide*, NIST SP 800-61r2 (2012); NAT'L INSTITUTE OF STANDARDS AND TECHNOLOGY, *Incident Response Recommendations and Considerations for Cybersecurity Risk Management*, NIST SP 800-61r3 (2024).