Research Report

Second Quarterly
2021 Review

CYBER THEORY

CYBER THEORY

We are a full-service cybersecurity marketing advisory firm. We constantly collect and analyze the latest customer data segmented by security practitioner, industry and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona. With strategic insights from global education services, media providers, intelligence analysts, journalists and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompass all aspects of cybersecurity as well as the related fields of fraud, audit, compliance and risk management.

CONTACT INFORMATION

cybertheory.io

212.518.1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018

Table of Contents

01 The Second 90 Days
03 Money or Power
04 Takeaways
05 Nuclear Weapons
07 Playing Serious Games
09 Beyond the Surface
10 Chinese Ground's SITA
11 What's Old is New Again
13 Closer to Home
15 Healthcare under Siege
16 A Return to Pen and Paper
16 Across the Pond
17 Whats Been Hit
19 Speed of Acceleration
21 Bits and Pieces
22 IoT Landscape Threatening
23 Secrets in the Wild
25 Water, Anyone?
27 Thirds of System Operators Have No CISO
29 Judge Judy
30 Societal Impact
31 Eyes Wide Shut
33 So, Whats the Good News
35 One More Thing
36 Sharing Is Caring

The Second
90 Days

Following on the heels of a harrowing first quarter of this crazy year, the landscape became littered with even more detritus, left behind by an onslaught of ransomware hits, raising the stakes and targeting critical infrastructure.

The Kremlin continues to test both the strength and cunning of their attack teams and the preparedness and resilience of their chief adversary to the West.

Though it may seem like a while ago now, with all of the mainstream media coverage it received, the Colonial Pipeline attack was announced on May 7, 2021, and the follow-on news focused on whether Colonial would pay the ransom or refuse to cooperate with the thieves. As gasoline lines began to form all along the eastern seaboard, it became clear to the cybersecurity community that Colonial's OT was infected as well as their IT networks. Though they never admitted it.

It also became clear to those panicked and stranded in long gasoline lines filling plastic garbage bags with gas, that cyberattacks had suddenly become visceral and very kinetic.

Average walk-around citizens now knew what a cyberattack felt like and most who shared their views on social media were not anxious for more.

Refusing to describe either the origins or extent of the attack, Colonial finally knuckled under and after a couple of days, ponied up $4.4 million.

Subsequently, the FBI managed to showcase their skills at hacking crypto wallets and clawed back $2.3 million that had not yet been distributed out through the myriad of blockchain connections that the dark websters use to camouflage their laundering. In this case, DarkSide.

Money Or Power

Nonetheless, as we have repeatedly pointed out through our outreach, this attack was not about money, but rather about a demonstration of vulnerability and the ease with which a foreign national could bring down a key distribution system upon which we depend for every day convenience and facility.

Not to say the money wasn't part of the deal. It just wasn't part of Vladimir's deal. The ransom is the payout to the teams within DarkSide that the Kremlin directs to conduct these clandestine cyberattacks, and Putin is happy that they get paid from outside his own circle.

Many people are unaware that Putin owns 4.5% of the natural gas producer Gazprom, has a 37% stake in the Russian oil company Surgutneftegas and owns 50% of the Swiss oil-trader Gunvor. Using their most recent market capitalizations, Putin's combined ownership stakes would give him a personal net worth of $70 billion.

That puts him at 14th on the global rich list, just ahead of Steve Ballmer and Carlos Slim, and only $27 billion behind Zuckerberg. As the price of gas and oil have skyrocketed in the past 5 months, it will not take him long to close that gap.

Takeaways

Less than 30 days later, we saw JBS Foods get hit with a similar ransomware attack shutting down operations in Australia, Canada and the U.S., affecting thousands of workers.

How big a deal was that?

JBS is the world's largest meat supplier with more than 150 plants in 15 countries, employs more than 150,000 employees, and in the U.S. it processes nearly one-quarter of our beef and one-fifth of our pork. Vegetarians didn't care all that much, but meat eaters got hit with immediate scarcity and increased prices, and many people who subsist on a McDonald's diet were severely impacted.

Again, this attack was social experimentation, and had little to do with the $11 million paid to the Russian crime family. And, if anyone feels pretty good about their cybersecurity defenses and the degree to which their IT has been hardened against ransomware attacks, please note that JBS spends more than $200 million annually on IT and cybersecurity while it employs more than 850 IT and cybersecurity professionals globally.

Though you may spend, spending alone won't get you to the Promised Land.

WHAT DID WE LEARN FROM COLONIAL?

- Don't connect your IT networks with your IIoT networks.
- Stop using legacy VPNs, and particularly those with a single password, absent multi-factor authentication.
- Put someone in charge of information security and call her a CISO.
- Have a rehearsed and tested incident response and recovery plan in place.
- Call the FBI right away.

> Otherwise, these adversaries will continue to attack at will.

Nuclear Weapons

Just reported in the second week of June is another CI ransomware attack, this time on Sol Oriens, a subcontractor for the U.S. Department of Energy (DOE) that works on nuclear weapons with the National Nuclear Security Administration (NNSA).

REvil unabashedly takes credit for the attack with a message that claims, "The subcontractor did not take all necessary action to protect personal data of their employees and software development for partner companies. We hereby keep a right to forward all of the relevant documentation and data to military agencies of our choice, including all personal data of employees."

David Bishop, CISO of Trustwave, offered that we need "more serious repercussions" for this type of attack. "We're seeing advanced adversaries getting much bolder with who they are attacking, how they are blackmailing the targeted organization, and how they are monetizing their stolen goods."

"Most of these organized groups are financially motivated, but if these types of attackers shift their motivation from monetary to malicious, we should expect severe real-world outcomes," Bishop continued. "We've only seen the tip of the iceberg in terms of the real-world effects with the cyberattacks on JBS and Colonial Pipeline. The public and private sectors need to closely coordinate on what we can accomplish in terms of hard legal or offensive action to combat these threats – otherwise, these adversaries will continue to attack at will."

Playing
Serious Games

Adding additional fuel, the massive ($5 Billion) gaming company EA has also been hacked, during which game source code and related internal tools were stolen. The hackers, of course, made the announcement first, explaining that they managed to get away with the source code for FIFA 21, as well as code for its matchmaking server. The hackers also said they have obtained source code and tools for the Frostbite engine, which powers a number of EA games including Battlefield, Madden, Need for Speed and others.

Getting in by first infiltrating one of the company's communication channels, and for just $10, the hackers purchased a cookie that allowed them to join the company's Slack channel. They then posed as an employee to convince an IT administrator to grant them authentication to get into the company's corporate network.

With the skyrocketed technology complexity that is now so prevalent across all market segments, we now have so many ways to get into a target's network, it appears impossible to keep adversaries out. If it were golf match, I would have picked up after 7.

This attack highlights the vulnerabilities created by workplace communication technologies, which have exploded in popularity during the pandemic. We continue to rapidly adopt new technologies without any vetting or planning. Combine that with the switch to remote workspaces, and we have created brand new ways for cybercriminals to target organizations, yet very few companies have been able to adjust to the new reality.

The theft of source code will create a host of problems for the company, primarily because FIFA 21 has its own virtual currency, which itself is in high demand.

Game source code is highly proprietary and sensitive intellectual property that is the heartbeat of a company's service or offering. Exposing this data is like virtually taking its life and we have no idea at this point how this attack will ultimately impact the life blood of the company's gaming services down the line.

Beyond the Surface

While the motivations of the hackers appear to be strictly financial, the impact on EA's reputation could be serious. If, as many players suspect, the company has intentionally designed FIFA – one of its most popular titles – so that players who purchase coins have a better chance of winning matches and advancing their teams than players who do not, it could prove disastrous to the game's popularity.

$1.5B worth of FIFA coins were purchased by players in 2020.

Because EA game coins are bought and sold by players using real-world currency on unregulated market places like buyfifacoins.com, the hackers could be trying to attract the attention of organized hacker groups like China's Apt 41. With the source code, certificates and API keys in hand, Apt 41 could use them to mine coins and sell them in a process known as Gold Farming.

In 2015, the FBI arrested a group that had allegedly mined and sold $15 to $18M worth of this virtual currency by using vulnerabilities found in the game. Making profit off the in-game currency would be one of the most likely interests for the cybercriminals interested in purchasing the source code.

Access to the source would also allow someone to understand the game's functionality, its servers and logic, as well as undercover any secret algorithms and bypass anti-cheat technologies. With this knowledge, hackers could easily mine and sell the in-game currency.

The bad guys lifted 780 Gigs in total, which also includes all of the proprietary EA frameworks and software development kits (SDKs). As is often the case, these attacks are after one of the big four "P's": PII, PCI, PHI or IP. And in this case, the EA Intellectual Property (IP) is immediately fungible.

Chinese Ground's SITA

Air India's tag line, 'Truly Indian,' suddenly popped into the news in June when they announced a massive cyberattack by the Chinese nation-state threat actor, APT41.

Group-IB, with their Threat Intelligence & Attribution system being named one of the best in class by Gartner, Forrester and IDC are leading the investigation and have said that the current attack may have been a supply chain attack targeting SITA, but it is not the same attack the airline announced in May.

SITA is a multinational information technology company providing IT and telecommunication services to the air transportation industry.

The potential ramifications of this incident for the entire airline industry and carriers that might yet discover traces of the malware known as ColunmTK, based on the names of command-and-control (C2) server domains in their networks, are significant.

Group-IB's analysis has now revealed that at least since Feb. 23, an infected device inside Air India's network (named "SITASERVER4") communicated with a server hosting Cobalt Strike payloads dating all the way back to Dec. 11, 2020.

Following this initial compromise, the attackers are said to have established persistence and obtained passwords in order to pivot laterally to the broader network with the goal of gathering information inside the local network.

These back doors enable long-term, transparent data flows that appear to be legitimate under today's available technical scrutiny.

That earlier breach involved personally identifiable and PCI data reaching back to Aug. 26, 2011 and continuing on through Feb. 3, 2021. Those stolen records contained names, dates of birth, contact information, passport information, ticket information, Star Alliance and Air India frequent flyer data, as well as credit card data.

FireEye's Mandiant, which is assisting SITA with the incident response efforts, has since determined that the attack was highly sophisticated and that the tactics, techniques and procedures (TTPs) and compromise indicators point to a single well-known entity.

Group-IB claims proof that a server in Air India's network was hacked first, after it had established a connection to SITA's network.

We will watch how this expands within the airline industry and the interconnections with SITA. Once again, our network complexity creates substantial opportunities for digital explorers with bad intent.

What's Old is New Again

> "Identify the nodes and networks that should receive robust cyber and physical vulnerability assessments"

All of these supply chain, CI and ransomware cyberattacks are reminiscent of the findings in a 20 year old report entitled, "Protecting America's Critical Infrastructures: How Secure Are Government Computer Systems?" presented to the Congressional Subcommittee on Oversight and Investigations back in April of 2001, that offered in part, "America has long depended on a complex of systems – or critical infrastructures – to assure the delivery of services vital to its national defense, economic prosperity, and social well-being.

These infrastructures include telecommunications, water supplies, electric power, oil and gas, delivery and storage, banking and finance, transportation, and vital human and government services."

Aka, a target-rich environment.

And the report made the following recommendations: "Identify the nodes and networks that should receive robust cyber and physical vulnerability assessments; conduct near-term risk management assessments; justify funding requests for high-priority security enhancement measures in the areas of physical security, information system security, industrial security, emergency preparedness, counter-intelligence, counter-terrorism; and review actual business processes to better understand and improve the efficiencies of its organization's functions and information technology architectures."

Too little, too late, and maybe not at all.

Closer to Home

As the wave of cybercrime and cyberespionage rages on across all industries globally, on a more personal level, vulnerabilities in our connected world are expanding as well. CVE-2021-33887 is a published vulnerability in the Android Verified Boot (AVB) process for all devices relying upon Android operating systems.

Like for example, the Peloton, which has not been a stranger to front page news stories ever since reports of children and a pet being pulled, pinned and entrapped under the rear roller of the Tread+ treadmill, leading to the death of one child.

McAfee researchers described a worst-case scenario where an attacker could boot the Peloton with a modified image to gain elevated privileges and then leverage those privileges to establish a reverse shell, granting the attacker unfettered root access on the bike remotely. The hacker could then tamper with the product at any point from construction to warehouse to delivery, installing a backdoor into the Android tablet that comes with the bike without the end-user knowing.

An attacker could also walk up to a Peloton bike installed in a gym and perform an attack, gaining root access on these devices for later use.

While topical, because of all the high-profile people who use Pelotons – including the POTUS and first lady – the AVB vulnerability isn't unique to Peloton. Any and all Android bootloader security settings need to be configured properly by the manufacturer, or a bad actor can gain complete control of the bootloader and the device, whatever it may be.

In the case of Peloton however, their camera, microphone and local network access make it a particularly attractive target.

In our new WFH world, those elements easily serve as a pivot point to access other devices connected to the home network and tangentially, the enterprise network connected through the same router. The threat landscape then expands to include covertly listening in on virtual meetings and other sensitive business conversations that now take place away from a centralized physical office location.

And further expansion can easily occur within any OT or IoT setting when the base OS for a connected device is Android-based and connected to, for instance, an IoMT device in a hospital where many medical devices run on Android operating systems.
It's only a matter of time before we start seeing increasing deadly attacks within our highly vulnerable healthcare providers.

Healthcare under Siege

To the exact point, Stillwater Medical Center was hit with a ransomware attack on June 13 and is currently operating under electronic health record downtime as it attempts to bring its systems back online. The health system operates a number of care sites, specialist offices, hospitals and clinics in Oklahoma.

In the immediate wake of the attack, Stillwater experienced major disruptions of its phone systems, and patients were urged to call 911 instead. There were also reports of a broken online patient portal, and associated email system as well.

A late update on June 15 indicates that the phone service continues to be working only intermittently throughout the entire health system.

The Stillwater attack occurs right after another cyberattack on two University of Florida Health hospitals, whose systems remain offline and inaccessible two weeks later. The Villages Regional Hospital with over 130,000 residents in their retirement community was attacked alongside Leesburg Hospital, on May 31, and both have been operating under downtime procedures since then.

A Return to Pen and Paper

Following all of these attacks, hospital clinicians have been documenting all patient care with pen and paper.

The increased physical danger arises out of the absence of reliable and immediate EHR access, which puts patients at risk for unverifiable allergies or potential drugs to avoid. Clinicians have reported that the system outages have caused patients to either miss medications or to receive the wrong prescription.

The hospital staff is calling pharmacies directly to verify patient prescription histories. There have also been reports of staff inadvertently matching patients with the wrong lab chart. The outages have also caused long delays in the receipt of lab reports.

Across the Pond

Further from home, the Ireland Health Service Executive (HSE), Ireland's largest public health system, is still trying to bring its systems back online after a significant ransomware attack took their networks down on May 14.

One month later, HSE continues to insist that patients bring their PHI with them to the emergency department, including medical records and patient chart numbers, medications and any previous discharge summaries. The impact on efficient patient care has been immeasurable, as only urgent care for life-threatening conditions is being provided through the emergency center, and all out-patient care has been cancelled.

What’s Been Hit?

The radiology and medical imaging departments across all sites appear to have been the hardest hit by the attack. Immediately following the attack, appointments for those departments were canceled.

“Notwithstanding the substantial technical recovery and improved operational capacity, it’s evident that information and communications technology (ICT) and clinical communication systems fall short of what is required to work safely and deliver care at an acceptable level of risk,” HSE Chief Clinical Officer Colm Henry, MD, explained to staff.

“In most instances workarounds remain in place,” he added. “Major ICT systems such as NIMIS, Apex and ICM have been restored, but not to the level required to provide system integration and seamless clinical communication. It remains the case that recovery of ICT systems is not synonymous with service recovery.”

As the HSE recovery team continues to work around the clock, uploading backlogs and reconciling patient records, cleansing and rebuilding systems, they’ve discovered an alarming number of systems and devices that have been destroyed beyond repair.

New Zealand Waikato DHB remains in EHR downtime, one month after their attack.

More than one month after a ransomware attack struck multiple hospitals of the Waikato District Health Board (DHB) in New Zealand, their IT team is still attempting to bring IT services back online.

Clinicians are continuing to operate EHR downtime procedures using pen and paper to record patient interactions and have hired hundreds of additional IT workers to assist with recovery efforts, while refusing to pay the attackers’ demands.

So far, one month later, they have been able to restore about 20% of its workstation network and more than half of its servers. Reports from on-site clinicians and staff members showed the cyberattack caused chaos at the impacted hospitals. Providers have been unable to send X-ray images between departments, access patient notes or access patient records.

In other words, not only is it not slowing down, it is increasing dramatically.

Speed of Acceleration

In the first half of 2021, so far, ransomware attacks have brought down the network of multiple providers, including Scripps Health; Rehoboth McKinley Christian Hospital in Gallup, New Mexico; Arizona-based Cochise Eye and Laser; St. Margaret's Health - Spring Valley, Allergy Partners in North Carolina, among others.

1,000 healthcare providers have been affected by ransomware attacks every week, reflecting a 7% cumulative increase on a month over month basis.

In other words, not only is it not slowing down, it is increasing dramatically.

While the Department of Homeland Security's CISA and NIST continue to publish and stress the adoption of best practice defense and mitigation measures, much more can and has to be done by our Federal agencies to step onto this battlefield.

Because the threats to human life elevate the conversation to a national security level issue, and healthcare providers cannot alone defend themselves from this storm of incoming.

Perhaps our newest members of the federal cybersecurity team, Chris Inglis and Jen Easterly, will have an immediate impact on this sector with new support and a takeover of the cybersecurity infrastructure for healthcare providers.

Radical?

Indeed.

Bits and Pieces

In May, the mortgage settlement giant First American Financial Corp. was discovered to be leaking more than 800 million documents, many containing sensitive PII/financial data, related to real estate transactions dating back 16 years.

In the second week of June, the SEC settled its investigation after First American agreed to pay a penalty of less than $500,000. Since they generate $6.2 Billion in revenue, the penalty was as insignificant as coffee money. Without fiscal consequence or ramifications, why should anyone spend millions on cybersecurity technologies? $500K is simply a no brainer, risk transfer.

This is the equivalent of the fox in charge of the hen house. If the SEC can't insist on penalties that are commensurate to the crime, we will never escape the rinse and repeat cycle for cybercrime in the financial sector.

Not because the Wall Street leaders are bad actors, but rather because the same folks are great business people.

IoT Landscape Threatening

ODA is a nonprofit organization that creates SDKs for engineering applications, including CAD, GIS, building and construction, product lifecycle management (PLM), and IoT. Their website claims 1,200 member companies worldwide, and its products are used by folks like Siemens, Microsoft, Bentley and Epic Games.

It turns out that ODA's Drawings SDK, which is designed to provide access to all data design files, is affected by several vulnerabilities that can be exploited by convincing the targeted user to open a specially crafted file.

The vulnerabilities, rated high and medium severity, can be exploited to cause a denial of service (DoS) condition, execute arbitrary code, or obtain potentially sensitive information by getting the targeted user to open specially crafted DWG or DGN files with an application that uses the SDK.

ODA, in defense, has noted that in order to be able to take complete control of a system, an attacker would need to chain one of the code execution vulnerabilities with a privilege escalation flaw. So, it's not a real big cybersecurity threat.

Except that the same technique was leveraged through SolarWinds' vulnerabilities and that cyberattack didn't turn out so well for the good guys.

Secrets in the Wild

The South Korean Atomic Energy Research Institute (KAERI) was hacked on May 14 by the NoKo bad guys, aka the Kimsuky group. CISA has recognized the group as a global intelligence gathering team that has targeted South Korean COVID-19 vaccine researchers and nuclear reactors.

The group often uses phishing to mimic websites like Gmail and Outlook. Then they install an Android and Windows backdoor called "AppleSeed" to collect information.

A vulnerability in a … wait for it … VPN used by KAERI allowed access to one of the agency's servers before they could detect, block the IP addresses and install security patches. The KAERI network was breached using an email address from President Moon Jae-in's former advisor, Moon Chung-in, that was acquired during a 2018 Kimsuky-attributed cyberattack almost three years earlier.

Proving once again that just because nothing apparently happens following a cyberattack, doesn't mean there won't be downstream damage. Imagine bringing your cyber insurer a claim for a hack that occurred 3 years ago when your computing environment was completely different and multiple risk assessments had been conducted since.

Officials fear that the leaking of information pertaining to nuclear technology, like reactors and fuel rods, could pose security risks, and this attack may be part of a larger ongoing campaign. Malwarebytes, in early June, reported several attacks on South Korean universities, government officials and companies in South Korea, and attributed them to Kimsuky.

When we don't hear about these attacks in our news feeds, we often feel like the world is not as scary as we thought, but we'd be wrong. There is more cybersecurity action occurring in the South China Sea than in all of Western Europe, as four countries jockey for position on the global stage. The end may well usher in with a bang, over a whisper, and whichever way it goes, U.S. interests are closely tied to all four countries.

Water, Anyone?

A June survey conducted by the Water Information Sharing and Analysis Center (Water-ISAC) and the Water Sector Coordinating Council tries to assess the state of cyber preparedness among 606 water and wastewater utilities.

These represented approximately 52,000 community water systems and 16,000 wastewater systems in the U.S., and the general findings were that the water industry demonstrated a range of cybersecurity preparedness, ranging from a little to none.

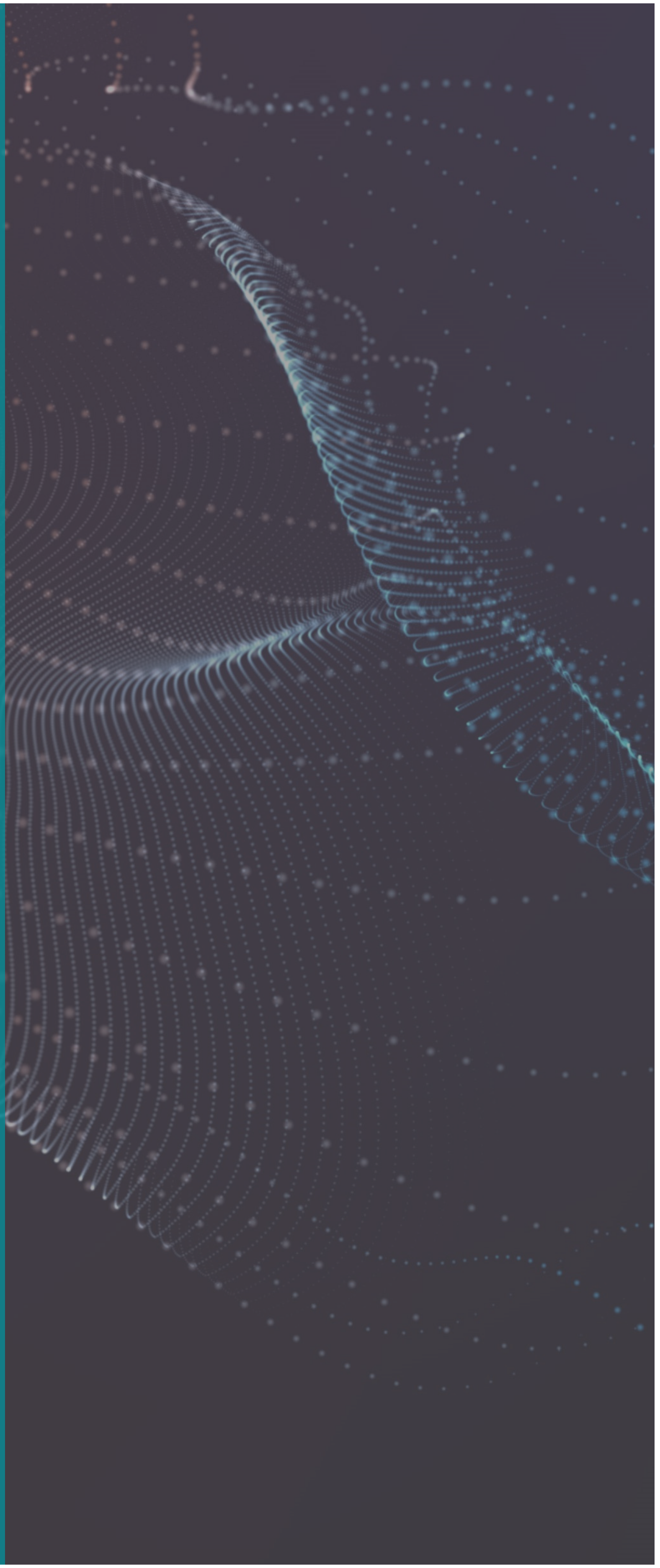
Many of the utilities self-assessed as “subject to economic disadvantages typical of rural and urban communities,” while other don’t have access to a cybersecurity workforce.

Regardless of excuse category, almost all of these utilities are struggling to maintain and replace infrastructure, comply with safe and clean water regulations, while still being able to maintain their necessary levels of profitability.

More than 60% of water utilities say they have not fully identified IT assets in their networks, and only a little more than 21% of those utilities said they are working to do so. Roughly 70% said they have not fully identified all OT assets and fewer than a quarter are working to do so.

Why did it take a near miss in Oldsmar, Florida following an earlier discovered attempt at poisoning a water treatment plant in Oakland using the same TeamViewer vulnerability before this essential lifeline came into focus as a critical infrastructure threat with national security implications?

> “Roughly 70% said they have not fully identified all OT assets and fewer than a quarter are working to do so.”



Two-Thirds of System Operators Have No CISO

Sixty-four percent of respondents said their utility does not employ a chief information security officer.

That Oakland incident, which was previously unreported, is one of many of the hundreds of treatment plants that responded they were “not sure” if they had experienced an incident. The Water-ISAC published a list of six older CVEs for its members on June 17, saying it was “aware of several reports of threat actors leveraging multiple vulnerabilities to exploit unpatched systems in the water and wastewater sector.”

The continuing risk assessment and evaluation of our water and pipeline systems falls remarkably under the EPA and the TSA, neither of whom have experience dealing with cybersecurity issues nor have enforcement authority over cybersecurity lapses.

Their purview is limited to best practice recommendations which are not followed by many, and in the case of energy, a senior TSA official in 2019 testified to lawmakers that the office responsible for securing the nation’s pipelines – the surface division in the office of security policy and industry engagement – has only five full-time employees, none of whom are cybersecurity experts, to watch over 2+ million miles of energy pipeline.

And as we try to turn the page on June, we learned that on the 21st, another attack on a water district player has been discovered. The Metropolitan Water District of Southern California has been hacked by Chinese-backed hackers leveraging security vulnerabilities in the Pulse Connect Secure appliances, namely their VPN which is notoriously porous. MWDSC provides water to 19 million people living in Los Angeles, Orange, Riverside, San Bernardino, San Diego and Ventura counties.

Security analysts say dozens of other high-value entities that have not yet been named, were also targeted as part of the breach of Pulse Secure, which is used by many companies and governments for secure remote access to their networks.

Mandiant Threat Intelligence assesses that Chinese cyberespionage activity has demonstrated a higher tolerance for risk and is less constrained by diplomatic pressures than previously characterized.

The CISA had warned of the potential threats faced by U.S. government agencies, critical infrastructure entities and other private sector organizations related to vulnerabilities in certain Ivanti Pulse Connect Secure appliances, a widely used SSL remote access solution. The exploitation of these vulnerabilities could allow an attacker to place webshells on the appliance to gain persistent system access into the appliance operating the vulnerable software.

CISA and the folks at MITRE ATT&CK can warn until the cows come home, but if no one is listening, we will continue to watch these attacks, now emboldened as they discover a target rich environment of unpatched opportunities and unmanaged and unprotected IIoT network infrastructures.

Judge Judy

No better example of multiple agency cluster dances than we have seen in the aftermath of the Colonial breach. Here we have the Department of Energy with the sector-specific agency for cybersecurity incidents, and its Cybersecurity, Energy Security and Emergency Response (CESER) office, which is managing response. CISA is tracking the attack and publishing regular bulletins to industry about guarding against ransomware. The FBI is investigating as well. There have been several pushes in Congress over the years to clarify or shift responsibilities, but those bills ultimately failed.

I don't care whether congressmen can't figure out how Facebook makes money, but I DO care that these same law makers continually look the other way, rather than confess their ignorance and seek an understanding of the growing threats to our National Critical Infrastructure and pass some legislation that will anger people and rustle feathers, but will also impose rules and consequences for the continual brushing off of fiduciary responsibilities by system operators.

My vote?

Judge Judy.

Societal Impact

The heightened pace and frequency of supply chain and infrastructure attacks have pushed the topic out of the private professional domain and over into society as a whole. There is nothing like Eastern seaboard gas lines following aggressive moves by a new administration to redact the prior administration's rules on energy independence to incite the imagination of everyday citizens.

Yes, this cybersecurity business is a real problem and not just some ethereal threat casting about in space, the existence of which rivals UFOs in terms of national interest or concern.

Colonial changed all of that and its second act on JBS Foods brought the message home, not just to the constituency but to the White House and Congress as well.

The societal perception of cybersecurity before those two attacks was essentially fear, uncertainty and doubt, and completely disconnected from the realities of addressing it. Society has treated cybersecurity like a strange black box, with maybe a pulsing blue light on top.

Security experts are treated as mythical knowledge priests, but held far more weirdly than doctors or chemists, as regular folks just don't comprehend what these people actually do. Corporations give their CISOs lots of serious money, they weave some incomprehensible computer science together, the board reads reports that no one understands and everyone prays that nothing bad happens on their watch.

Over the first half of this year, we have so much breach data that says business decision making related to cyber risk is still seriously flawed, and when disconnected from the realities of business impact, leads to serious business harm. Our executives are distracted by compliance, the latest hackers and their techniques, and how much they are spending on cybersecurity defense.

Eyes Wide Shut

In addition, we have seen an increase in aggression and confidence on behalf of our adversaries. All of the serious strikes we have discussed in both quarterly reviews this year have taken the zero day concept to new heights and spawned a new level of maturity among threat actors.

Now that we are paying attention, we notice many more attacks on infrastructure, especially water supplies and the systems that manage them. Ransomware attacks have come into focus now that the voting public is witnessing first hand, the enormous pay-outs that were rarely seen even 2 years ago.

This now thriving business model, as attested to by bad folks like DarkSide, reveal their dark web presence resembling a consumer products campaign with press releases, YouTube 'how to' videos, a full-on tech support desk, financial planning, payment processing, negotiation proxies and user guides as bonuses.

DarkSide alone has earned just under $100 million in 2021 thus far.

Their business model is now what is known as Ransomware as a Service, in which the malware developer charges a user fee based on a sliding scale that runs 25% for any ransoms less than $500,000, and escalating down to 10% for ransoms over $5 million.

With that level of support, even small-time criminal franchisee syndicates and hackers with only mediocre computer capabilities can pose a national security threat.

American journalist Megyn Kelly interviewed Putin in 2018 and pressed him on why Russia was looking the other way while hackers actively interfered in the American election, so he tried to remind her that there was nothing to arrest them for.

“If they did not break Russian law, there is nothing to prosecute them for in Russia,” Putin said. “You must finally realize that people in Russia live by Russian laws, not by American ones.”

So, What's the **Good News?**

The federal government has awakened to cybersecurity threats and the need for the Fed to step in and provide some centralized control over the theater. How and when they are able to organize to do this is anyone's guess, and while it is way too late for us to start catching up to our adversaries, I will always take late over never.

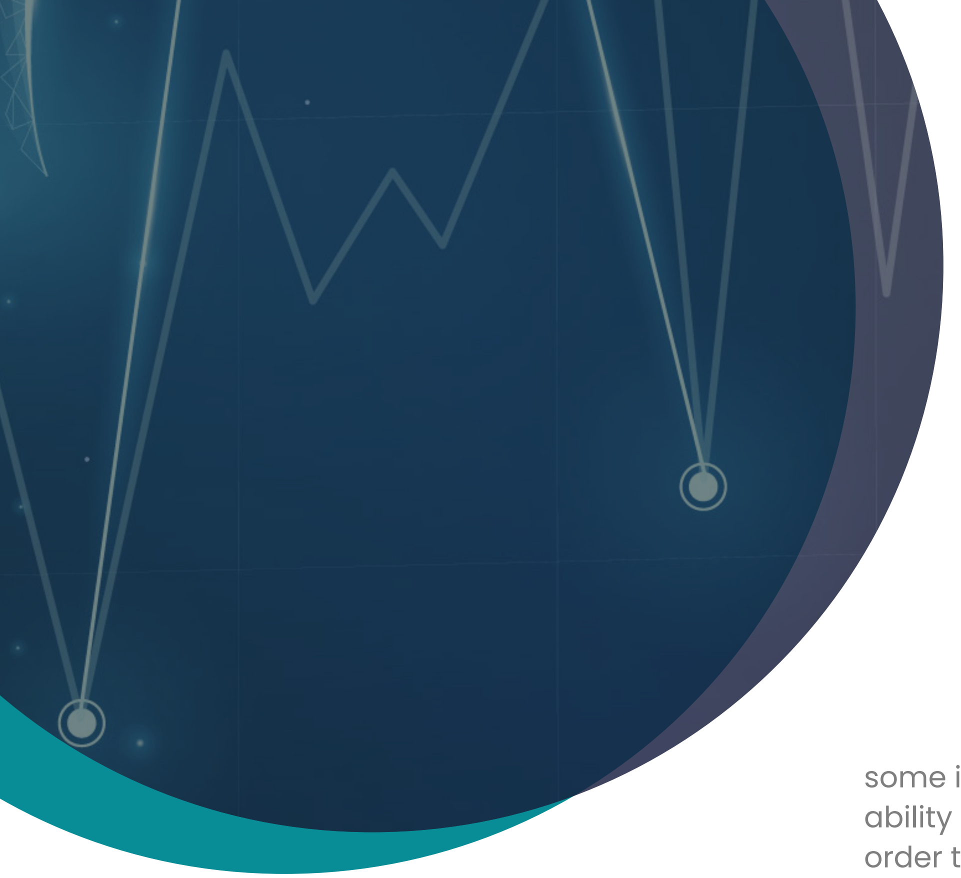
Setting aside the inadequate funding for cybersecurity R&D, we now have a couple of 90 day plans, an executive order that is stressing Zero Trust and compliance mandates, new blood in senior positions within the security hierarchy and some very talented folks in positions of authority.

While some wise man once said that our single greatest talent in America is creating bureaucracy, we also managed to create a weapon of mass destruction from some loose atomic science in only 27 months, and in 8 short years we went from walking around on earth to walking around on the moon – and returning back.

We have some of the brightest and best cybersecurity practitioners working hard to create innovative software, network and hardware solutions to very specific security challenges. We are rushing to apply AI and machine learning to these products and creating breakthroughs in hard problems on a daily basis.

We have created a technologically dependent digital world where the U.S. is the most advanced in terms of adoption of the technology for advances in science and medicine, construction and telecommunications, biology and chemistry, mathematics and engineering and as a result, we have wrapped ourselves in the glassiest of glass houses (a shameless lift of a (ret.) General Keith Alexander quote). We operate the controls at great risk. With hope and confidence, we look toward the next quarter.

Let's see what it brings.



One More Thing

Looking back two years to the spring of 2019, a multinational manufacturing company named Norsk Hydro, a big International player in the global aluminum manufacturing supply chain got seriously hacked.

Lacking a corporate website, they had to use their Facebook account to notify folks, and of their 160 offices globally, most had to conduct everyday business without any digital infrastructure – they communicated via fax, pen and paper.

The culprit?

LockerGoga, a ransomware that exhibits some interesting behaviors, including the ability to spawn different processes in order to accelerate the file encryption in the system. Its execution depends upon launching from a privileged account, it creates multiple slave processes on the endpoints to encrypt its target files, and then it locks all users out by changing all credentials to dead destinations.

A month prior, a huge French IT services company called Altran was hit and completely crippled by the same ransomware.

Altran never said a word. To anyone.

Barely a word emerged in the media about LockerGoga. And consequently, not one cybersecurity product vendor flagged the file as malicious. Immediately following the Norsk attack, two U.S. chemical manufacturing companies were attacked using the same malware, without subsequent disclosure.

There are so many gaps and holes in our cybersecurity ecosystem, it is often hard to decide where to start. Non-disclosure however is a great candidate.

Sharing is Caring

Contrary to some popular sentiment, our cybersecurity vendor community does an admirable job of issuing patches for vulnerabilities rapidly after they are discovered and generally offer full disclosure around exploits.

But if attack victims keep this stuff secret, we are allowing the threats to continue without the ability to warn downstream victims against similar attacks. We need to stop worrying selfishly about reputational impact and start publishing these things as soon as possible following an event, along with technical details around the attack vector. It is no longer unusual for an organization to be breached and in fact, those who haven't yet been breached are beginning to appear conspicuous by their absence.

The United Kingdom has a National Cyber Security Centre's Information Sharing Partnership and it is working well, generating the expected dividends and we need to follow its act.

It is long past the time to continue allowing individual organizations to make their own decisions about what is to be reported and when. We need global requirements and standards for private disclosure along with the free flow of technical information to trusted examiners.

But with a quid-pro-quo that the government will shield the reporting company from blow back in the form of class-action lawsuits and claims of contributory negligence, along with a return of capital in the event a ransomware payment must be made (ala, Colonial Pipeline, who will soon be facing both legal issues amid scores of class action suits).

Had not Colonial paid that ransom demand, their OT systems were surely compromised and no transportation fuel would have flowed to all of those destinations up and down the eastern seaboard.

While information sharing and cooperative investigative initiatives will not put an end to ransomware, they surely will enable some denting of the armor.

And boy, could we use some of that.

CYBER
THEORY

cybertheory.io
212.518.1579 • info@cybertheory.io
530 7th Avenue, New York, NY 10018