END OF YEAR ANNUAL SUMMARY

2021 REPORT

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 to perform 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 encompasses 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

> “Ransomware attack encrypted the data of more than 1,000 Kaseya VSA customers”

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

2021 The Year of Complexity

Wow. What a year!

We began last January with the realization that we have met a new and far more difficult class of cyber threat with the SolarWinds attack followed by the Colonial Pipeline attack in May. Both point to a fully wired world where physical and digital are colliding at unprecedented speeds.

If we had to choose a theme for 2021, it would be complexity. The convergence of internet-enabled computing devices across multiple cloud entities and configurations, the rapid acceleration in the growth of “smart” devices and their interconnectivity, the push toward Continuous Introduction/Continuous Delivery (CI/CD) for more agile and shorter innovation development cycles craved by business units and customers have all combined to create a perfect storm.

That storm has led to compromised foundational systems and porous supply chains virtually begging for bad guys to attack their multiplying points of vulnerability. We continue to increase the number of weakest links as almost every new layer or modification brings along with it not just our supply-chains but also new vulnerabilities and easily exploitable holes back into the backbone of our network systems.

Colonial was followed by a similar attack on Iran and others around the globe, where attackers have gone after physical infrastructure targets with abandon – ransomware has continued to grow in popularity with attacks on insurance companies like CNA Financials, one of the largest in the U.S. The company paid $40 million to get its systems and data back, yet this was only a brief highlight along the way to record ransomware attacks around the world.

The volume and frequency of these attacks has caused observers to scratch their heads in disbelief over the lack of response by not just companies in the Fortune 500, but all companies whose data is important to their daily business operations.

Why we continue to try and defend against increasingly sophisticated attacks with the same, conventional defense in depth mindset is beyond reason to fathom.

We will resist the urge to throw in a plug for Zero Trust here, but it is indeed, one strategy that will mitigate and reduce the number and damage that cyberattacks can cause. But, it is not a strategy that is being embraced presently by most companies. This goes toward education and a surfeit of misleading information and marketing propaganda, but some of us are working hard to reverse that course through the creation of the CyberTheory Institute and its maiden initiative around Zero Trust.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Ransomware Abounds

Without enumerating the attacks themselves, because most companies don't want the attention and fail to report them, we witnessed ransomware attacks from just six ransomware gangs responsible for cybersecurity defense breaches in 292 organizations who actually reported them and well above $100 million in ransomware money alone, not counting the hundreds more spent recovering their data and systems.

In 2020, we saw criminal organizations steal more than $45 million in ransom money, while imposing a huge financial impact on the healthcare sector along the way, with over $20 billion lost in impacted revenue, lawsuits and ransom payments. Over the course of that year, over 600 hospitals, clinics, and other healthcare organizations were impacted by 92 ransomware attacks. But, 2021 was worse.

In 2021, we watched as JBS Foods, Brenntag (chemical distribution) and Acer got whacked, and those three firms ponied up over $65 million in ransom alone.

An example of the back stage pass only attack is Quanta, one of Apple's biggest business partners, where in April, the notorious REvil gang attacked and demanded $50 million. When Quanta refused to pay, REvil targeted Apple and stole product blueprints, some of which they leaked as proof of life, and subsequently REvil was either paid off or called off. The data is not clear. But, either way, they got what they wanted.

Apple and Quanta did not. You didn't hear about it because neither wanted it reported.

"In 2021, we watched as JBS Foods, Brenntag (chemical distribution) and Acer got whacked, and those three firms ponied up over $65 million in ransom alone."

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Flurry of

Executive Orders

With a flurry of executive orders back in the spring, the Biden administration sought to stem the rise in cybercrime by insisting that companies who do business with the Federal Government, abide by some tight rules regarding security fundamentals and Zero Trust in particular.

The hope is that these executive orders will force companies who manufacture and distribute software to closely examine their supply chain to detail what is actually coded and to thoroughly vet any open-source software that is part of the supply chain. The attempt is wrapped around the demand that all software companies are reviewing their source code along with their open-source dependencies – since today's software uses over 85% open-source, with countless unknown downstream dependencies, the task will be virtually impossible.

One single component of that order is the fully transparent disclosure (SBOM) of their entire source code libraries to buyers, which is not only flawed, but impossible to legislate. In theory, because you will have visibility into the provider's source code, you will be able to see flaws and vulnerabilities.

Vaguely interesting but not effective.

It would not have prevented the SolarWinds disaster, because the hacks happened at compile time, inserting the malware in a single line of code at object-build and undetectable as well. What the SBOM WILL do however, is to add yet another layer of compliance to an over-worked and under-resourced business function who has neither time nor skilled staff to manage such a process. But it by itself, will not prevent the next SolarWinds attack.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Data Publicity

Fast forward through the May discovery that the personal data of more than 100 million Android users was exposed due to multiple hyper-cloud server misconfigurations, and unprotected in real-time databases used by 23 apps, the thefts ranged from 10,000 to 10 million and included internal developer resources, and other not widely reported information.

Of the 23 apps analyzed, a dozen had more than 10 million installations on Google Play and the misconfigurations demonstrate a lack of basic security practices in the applications' deployment practices. Surprise? Nope.

In August, an unprotected Thailand travel open-source Elasticsearch database was discovered to have been fully compromised with data dating back ten years, containing the PII of more than 106 million international travelers, including passport numbers, visa types and card numbers. The Thai authorities acknowledged the theft and restored a secured version of the data base a day after being alerted. A day too late.

In June, we discovered that the Iranian business and social messaging application Raychat had suffered a large data breach which exposed millions of user records and subsequently destroyed the application by a bot-orchestrated cyberattack.

Raychat had stored its user data on an open-source misconfigured MongoDB database that left the data vulnerable. In spite of the fact that we know several NoSQL databases like Mongo are targets for bot attacks operated by malicious actors who scan the internet for open and unprotected data, we insist on using them anyway.

Then there were Stripchat, Socialarks and Bykea, all using Elasticsearch databases, resulting in hundreds of millions of leaked profiles obtained from Facebook, Instagram and LinkedIn database scrapings. Those worried about data privacy can stop now. And it is hardly Facebook's fault alone. Your PII is all over the dark web right now, either sitting inside dossiers combined with PHI data obtained from a rash of earlier hospital and healthcare breaches over the last two years or sitting alone in a credit card cache as part of securitized small lots available for sale to investors.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Dark Wilderness of Personal Data

Even without the help from scarpers, Facebook and LinkedIn combined to provide over one billion accounts directly.

The Facebook breach put 533 million accounts belonging to Facebook users from 106 countries, including more than 32 million records on users in the U.S., 11 million on users in the U.K. and 6 million on users in India out into the dark wilderness. Samples of the leaked data confirmed that Facebook users' phone numbers with email addresses were included. If you haven't been socially engineered yet, you will be soon.

LinkedIn's contribution was phone numbers, email accounts, usernames and physical addresses of over 700 million members. Identity masquerading will soar in 2022.

But, hands down, the Elasticsearch open-source winner this year was Cognyte, a cybersecurity analytics firm that ironically provides a cyber intelligence service that is used to alert customers to third-party data exposures. Stored on their Elasticsearch cluster, the master database contained 5,085,132,102 records. Yes, that's billion.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved
Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Critical Vulnerability in
Critical Infrastructure

On the OT side of the coin, things may be actually worse.

Colonial, NEW Coop Agricultural Distribution, JBS Foods, Molson/Coors, and the Oldsmar, Florida water treatment facility illustrate the attacker-appeal of poorly protected ICS and Industrial Automation systems and the fragility of critical infrastructure and manufacturing environments that are exposed to the internet.

Why?

637 ICS vulnerabilities were disclosed in the first half 2021, a 41% increase from the 449 vulnerabilities disclosed in the second half of 2020. Eighty-one percent of those were discovered by sources external to the affected vendor, including third-party companies, independent researchers, academics and other research groups.

Seventy-one percent of the vulnerabilities are classified as high or critical, 90% have low attack complexity, 74% do not require privileges and 66% do not require user interaction, such as opening an email, clicking on links or attachments, or sharing sensitive personal or financial information.

In addition, 61% are remotely exploitable, and wait for it … 65% may cause total loss of availability, while 26% have either no available fix or only a partial remediation.

Zero Trust?

Of course.

ICS-CERT has issued the top recommended mitigation steps which include network segmentation (applies to 59% of vulnerabilities), secure remote access (53%), and ransomware, phishing, and spam protection (33%). All of which are accomplished through Zero Trust design principles.

But the crazy disconnect may be research from Skybox Security that tells us 83% of organizations suffered an operational technology (OT) cybersecurity breach in the prior 36 months, yet 73% of CIOs and CISOs remain “highly confident” their organizations will not suffer an OT breach in the next year.

Apparently, one of the missing links in cybersecurity training and education is how to accept reality when it pounds you in the face and what to do about it that is different than what we have done in the past.

I realize I am leaving out Kaseya Coop, the Swedish supermarket chain, and the NBA to name only a few. Companies like Johnson & Johnson experience 15.5 billion cybersecurity incidents on a daily basis. Also, COX Media Group, Accellion, Pandora, Astoria, ParkMobile, ClearVoice, Bonobos, Kroger, Parlor, VW, Audi and dozens of healthcare providers add to the roster of catastrophic breaches in 2021.

So, we could list them all, but what point would we make other than the point we already have made, that cyberattacks are increasing daily and we increasingly don’t have the will to address either end of the funnel (defense or digitalization) with proper discipline.

Will it continue into 2022?

Bet the mortgage.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved
Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

One Last

Honorable Mention

One last breach just discovered in the closing moments of 2021 deserves mention however, in that it is a living example of the absence of hygiene, and due care and the broadening target value. D.W. Morgan, a multinational supply chain management and logistics company based in the United States, left an Amazon S3 bucket open without authorization controls, exposing sensitive data relating to shipments and the company's clients.

As the market leader, D.W. Morgan, a $240 million logistics company provides services to some of the biggest companies in the world and all of their data, including IP is lying exposed on the Internet. It is the exact same breach that cost Capital One over a hundred million 2 years ago. In this case, more than 2.5 million files were exposed containing transportation plans and agreements outlining every step of the shipment process for each exposed D.W. Morgan client, including huge companies like Cisco and Ericsson.

That data represents shipping instructions and full PII for every Morgan employee, client employee and ship to employee involved in each transaction. Which opens the doors to a myriad of scams and fraud, but in particular, cybercriminals could directly contact client businesses and their employees, referencing shipment details to build trust. From there, hackers could target employees and client businesses with various scams, like the fake invoice scheme.

With invoice details, bad guys will have no trouble convincing harrowed WFH employees that extra charges or half or all of the invoice value must be paid prior to completion of the shipment. Since client employees had their full names and contact details exposed, the attackers could call or message, referencing details of shipments (like prices or goods ordered) to masquerade as a colleague, D.W. employee or a representative of a supplier. Once the client employee trusts the hacker, the attacker could also convince them to click on a malicious link.

D.W. Morgan's third-party suppliers have had their details exposed, too, which means hackers can expand their phishing to many additional organizations. What is inside an attack is not always obvious to the industry observer and some of these repercussions will manifest themselves later as they emerge from the long tail following this primary attack.

This swarm effect will continue throughout 2022 as complexity expands, hygiene suffers, APIs dominate, open-source continues to carry the programming load, more data and processing is pushed to the hybrid cloud and fewer companies will be able to cope with an overwhelming enemy force.

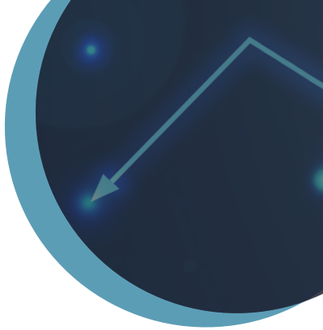
Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved
Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Not-So-Great Expectations

Having said that, we don't like predictions.

They are either too Captain Obvious and safe to make, or too fanciful to imagine properly. But it would be fair to find out what our expectations, based on our research for next year might look like.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved



So, here's our top-ten list:

1. Physical infrastructure will top the list of dangerous attacks with serious outcomes
2. Double-extortion ransomware attacks like the one just imposed on Shutterfly will continue
3. Open-source supply-chain attacks will continue to grow with no solution in sight
4. Folks will continue to accelerate the use of open-source database management systems
5. As Web App attacks skyrocket, we will see a rush to protect APIs
6. Active Directory will continue to dominate as the world's most powerful Trojan
7. Windows and O365 will remain the most vulnerable and porous targets for attackers
8. Complexity will continue to increase, exacerbated by hybrid cloud storage, APIs and 5G
9. The skills gap will widen even more dramatically than in the past
10. The global geo-political stage will be dominated by cyberattack scenarios in real-time

The good news?

There are things we can do.

From our director, Steve King's upcoming book, "The Zero Trust Field Handbook: How We Can Reverse the Attacker/Defender Dynamic on the Five Battlefields of Cybersecurity," here are a few suggestions:

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Closing the Skills Gap

Let's spend $60,000,000 in new tax-payer dollars on a National Cybersecurity Master's Education program where we invite 500,000 college graduates with undergraduate degrees in engineering, math and science to participate in a fully funded, 2-year graduate program focused on building cyber-warrior skills. When I say fully funded, I mean $40,000 in tuition and $20,000 in living expenses each year. The entrance requirements would be similar to any graduate degree program in engineering, law or science at any leading university. Upon graduation, these students would be free to do what they want. Most would pursue a job in private industry. Some would become civil servants.

Others may abandon the profession altogether.

But we will have created a fast program that highly incentivizes participants, removes all reciprocal restrictions on post-graduation service and has a high probability of success.

The best part is that it will cost each U.S. taxpayer exactly $11.18. That is less than we spend on a standard Netflix subscription for one month. Let's get even crazier and throw in a $20,000 recruiting fee to help the graduates find a great job upon graduation. That will cost another $1.40 each.

That math is powered by 143 million taxpayers in 2020.

A simple program like this, with origins in Zero Trust thinking, run by our public and even private university systems, and not under the auspices of any government agencies, could quickly close the skills gap and flood hundreds of thousands of future CISOs and skilled cyber warriors into a thirsty market. Instead of bureaucrats and administrators, this brand of CISO would be trained in hand-to-hand cyber-enemy combat and equipped with the appropriate tools necessary to take the fight to the enemy, shifting the attacker-defender dynamic to offense and away from detect, respond and remediate.

We should supplement that with a purpose-driven cybersecurity education and training program that is offered on a just-in-time basis on-line, and delivered through a modern platform designed with the user experience as the top priority.

A program that has been vetted by CISOs and not a bunch of cybersecurity practitioners who drive curriculum creation through a necessarily narrow view of the landscape owing to their limited prior experience.

A program that delivers all levels of training, for cybersecurity practitioners, engineers, analysts, CISOs, non-CISO executive suite and board members, along with everyone else in an organization in a curated context that will insure everyone is getting exactly

what they need, when they need it, and in a consumable, consistent and repeatable set of programs overseen by an assigned success manager who assures that value is continuously extracted and applied.

An online learning program designed to be an extension of an organization's expanding purview over cybersecurity education, delivery, absorption and execution.
A program unlike any other on today's commercial markets, and one in harmony with NIST guidelines and the NICE framework that, in addition to preparing students for certification exams in over 150 specialties, can also bring outer dimensional thinking to the creation and building of new cybersecurity architectures and programs like Zero Trust, designed to move away from traditional, heritage programs and toward those best suited for modern cyberwarfare.

Much like the one we are building in CyberEd.io right now.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved
Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

National Service

Because we all now live in a digital world and cannot continue to ignore our individual responsibilities to manage our digital environments with dutiful care, it has been recommended that, in addition to the above described solutions, a model for a National Cybersecurity Service (NCS) program be mandated as a two-year public service requirement for every college graduate in the country – a wartime peace corps – less than half the service requirement for graduates of Annapolis – and/or 18 year olds who want to pursue a career path in cybersecurity without attending college.

The Israelis didn't manage to survive all these years by pretending their enemies were their trading partners. In much the same way as the IDF (Israeli Defense Forces) accommodates varying interests, our own NCS would offer different specialty educational opportunities, but the program concentration would be on a warrior-level and offensive cyber training.

Framed as a Manhattan project, such a program can be both authorized and funded by presidential order (ala FDR) and congressional mandate (though many would question whether any recent members of Congress would have either the political appetite or courage to do so). Regardless of cost, it would likely be dwarfed by legislation that we push through our law-making process on a daily basis and would be the only initiative aimed directly at a true existential threat, and one acting as a clear and present danger, and not just a measurable, abstract probability ten years into the future.

But if we don't do something really soon, it won't matter how many new technologies we invent, how much new cyber-threat awareness we create in our corporate boardrooms or how many new initiatives we create around the traditional approaches to managing cybersecurity. If we don't shift our approach to a risk management model, rebuild our cyber-defense infrastructure on the basis of a Zero Trust architecture, and staff it with an abundance of trained warriors, we will continue to retreat from this cyber warfront in the business of business, out-resourced, out-smarted and out-intimidated by opposing forces unencumbered by layers of social justice and political correctness, just as we have been doing for the last 20 years.

And at a national security level, all of the submarines, aircraft carriers, jet fighters or other military hardware and human resources we can muster against our enemies in some conventional theater of war won't matter either.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Advertising Our Vulnerabilities

Is it obvious that organizations with fewer references to cybersecurity in their annual reporting are less security mature and more likely to be breached? Or, is it more likely that cybersecurity is not high enough on the agenda for the board and executive to feature it in their flagship report?

With the annual report being such a significant communications tool, we can use it as an indicator as to the strength of the top-down security culture within an organization.

But so can our adversaries.

In a stunning example of this information asymmetry, we see that cybercriminals can follow a similar process as part of their open-source intelligence, identifying likely corporate victims perceived as the lowest hanging fruit. It is not a coincidence that Marriot, Anthem, Equifax, Yahoo, Home Depot, Sony, Adobe, etc., were among the many with the fewest references to cybersecurity in their pre-breach 10-Ks.

If we stay in denial and do nothing to change the course, in the next few years, the cybersecurity landscape will worsen significantly and any chance of protecting information assets, assuring truthful social media and providing data privacy will disappear completely.

Existential threats? Forget about Global Warming. Years from now, we all may all be speaking a different language.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Reverse Course

How can we reverse course and get ahead?

1. Change the reporting rules and prevent companies from reporting on their cyber vulnerabilities;
2. Apply granular controls over all Chinese-owned venture capital firms;
3. Stop using any products or services, including mobile devise and telecom, made in China;
4. Develop and apply rigorous process for fundamental hygiene with consequences;
5. Start sharing in earnest between public and private sectors;
6. Modernize our cyber laws to enable offensive security;
7. Mandate a Zero Trust migration for every computing environment within an aggressive timeframe;
8. Create and enforce national security mandates that specify technologies (not products) that must be part of every Zero Trust implementation;
9. Create the equivalent of a Manhattan project for the application of AI/ML to the problem space, with appropriate funding and speed to market;
10. Implement mandates on insurance providers to match coverage against a standardized NIST framework requirement.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

By removing excessive trust from our systems and networks, isolating our critical assets, ramping up the identity authentication process, and reducing the overall attack surface, we will have removed 50% of the breach risk, and made cybercriminals' jobs much harder.

By eliminating products and services provided by our number one adversary, we will put an end to pre-engineered leakage and impossible to detect hardware vulnerabilities.

By throwing the IP thieves out of our tents, we will stop the theft of the key technologies that our adversaries now use against us.

By reengineering the way we apply fundamental hygiene for patch and configuration management, we can decrease the number of vulnerabilities we now present.

By modernizing cybersecurity laws, we will remove the handcuffs that currently hinder law enforcement from apprehension and prosecution. In addition, we can open the doorways to a controlled offensive or forward defensive cybersecurity program at the national level, so that targets and victims can identify and seize bad actors in the process of committing their crimes.

By establishing mandated (vs. recommended) national security rules, we will assure that every organization is building and managing their IT and OT systems in accordance with best practices that have demonstrated their ability to increase resiliency while decreasing risk. One mandate can cover ransomware attacks, by preventing the payout, but also providing insured coverage for the damage recovery, adjusting for negligence and attendant liability, within a year of the attack under the jurisdiction of a special court.

By insisting on a mutual sharing of information and intelligence, private industry will have access to signals and behavioral data, now protected which will enrich new product design and development.

By instituting an aggressive AI/ML Manhattan project, we will be able to expand the concept of a YCombinator with a specific product focus, aggressive funding, curation and vetting and guidance from experts in those disciplines. It took only 4 years and $2 billion ($40 billion in 2022 dollars) to produce FatMan from whole cloth – it should take half that time and twice the money today.

By forcing insurers to provide and align their coverage against a standard for proper defense and controls, the burden is transferred to NAIC and FIO, forcing an actuarial proxy that will mature over time, yet set consistent expectations for both insurers and insured.

If we do all of this, will cybercrime come to an end? Will we reverse the asymmetry within our current attacker/defender dynamic? Will we achieve world peace?

Of course not, BUT ….

It will begin a reversal of course and shift momentum to our team.

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

Marketing

From a marketing point of view, we believe we may be on the brink of change in the way our industry typically allocates budget and the focus our programs and campaigns have traditionally taken. Many cybersecurity vendors are considering alternate approaches to marketing outreach, either through bespoke events or through media channels with video content, shot live, on location with cinematic scripts and narratives focused on stories and not on solutions or value.

That latter form of outreach comes as the recognition that conventional approaches, like whitepapers, eBooks and solution briefs, are failing to capture CISO attention. CISOs have no time for our messages and 17-page product explanations, and are under unprecedented pressure from zero-day disasters like Log4j. Now is not a good time to reach these folks.

More emphasis on brand awareness and authority and less on low-converting lead gen campaigns will provide sales uplift in 2022, as buyers are increasingly seeking informative entertainment and value those elements over feature and function. With the average number of point solution tools installed today exceeding 70, the IT environment is nobody's first rodeo. Buyers will buy based on factors we are not considering.

That shift will require bold courage on behalf of our marketers who will need to brave the results of ripping up yesterday's scripts and pioneering paths away from the thinking box. We are optimistic and confident that 2022 will

be the year of broadening awareness across a wide band of demographics, as more and more breaches target industrial control systems that manage the distribution of essential consumer products like food, water and energy.

What we do and how we do it, in both cybersecurity marketing and in cybersecurity defense, will be directional signals for both progress and regress in the years to come. The devil is in the details and there are many moving parts to these puzzles, but putting stakes in the ground for both how we defend (Zero Trust) and how we move markets (alternate messaging on alternate media channels), is a good place to start.
Happy New Year and all of our best wishes for 2022!

Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved
Copyright © 2021 CyberTheory, New York, NY USA | All Rights Reserved

CYBER THEORY

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