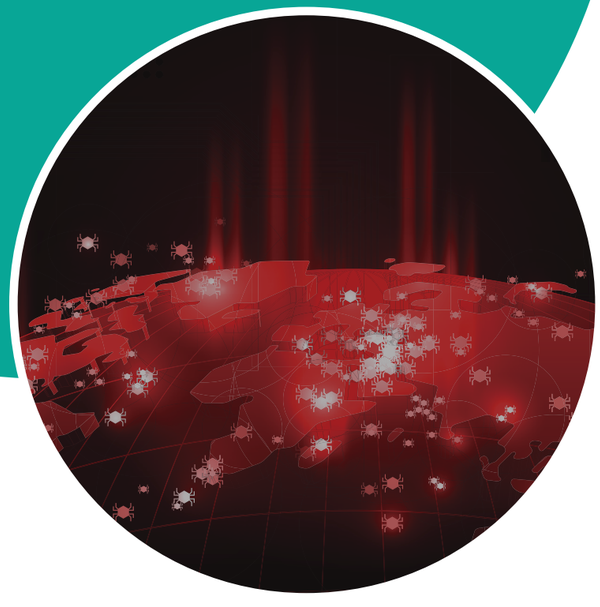
Research Report

First 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 INFROMATION

cybertheory.io

212.518.1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018

Table of Contents

The Last

90 Days

As we look back at our most recent breach activity during the last 90 days, we see a pattern emerging which is a departure from the historic norm, and one which likely portends a difficult future state. It is a state with which we are unprepared to assimilate, due to the 'protect and defend' architectural design of our cyber-defense technologies, combined with our constitutional guardrails and our confirmation biases toward our adversaries.

To wit, 99+% of our software tools are not engineered to detect or discover threat vectors like those used in the SolarWinds, Accellion and Microsoft attacks.

On top of that, our rule of law currently prevents the execution of offensive techniques and tactics outside our networks. We are also inclined to believe that cybercriminals are seeking immediate financial rewards (ransomw are)or the extraction of data which, when combined with other data, creates assets of value that can be sold on the dark web for delayed financial benefit.

It is also true that something deeply sinister is operating either in parallel or in place of those motivations. Something that is focused on intelligence gathering and channels of disruption, animated through cyber ops dis/mis/mal-information distribution and dissemination, and having little or nothing to do with financial gains. It is clear that the SolarWinds attack was a nation-state attack intent upon, and succeeding in, the disruption of our entire federal network infrastructure and resulting in the panicked response that followed.

Both Russia and China have shifted their positioning toward us in the ensuing weeks, with messaging that clearly conveys the sentiment that they no longer live in fear of their western adversary who has now been exposed to enjoy the latest version of the emperor's new clothing line.

Some in the media argue that this advance in acrimony results from the current administration's history of projecting weakness toward these two giants. While this may in some part contribute, I suspect instead that with the recent experiments in supply chain exploitation, they both feel comfortably confident in their cybersecurity skills.

The Future's So Bright,

They Gotta Wear Shades

As Kevin Mandia, the CEO of FireEye, pointed out during his congressional testimony, "Modifying the software build process, rather than the source code, means that this is a more portable attack and will show up in more places than just SolarWinds."

The key questions on the SolarWinds attack swirled around why so many public and private entities failed for months to detect the hack, and why only one of the tens of thousands of victims eventually found it.

After combing through tons of threat intelligence and forensics evidence, FireEye discovered the hack after it became a "stage two" victim.

Stage one entailed the bad guys compromising SolarWinds Inc. and its Orion software by the ghostly insertion of a backdoor into a software update. Stage two casualties are anyone who downloaded the legitimate, yet compromised, update that was infected during stage one.

Mandia also told Congress that he believed the attack required a multi-year preparation journey, and Microsoft President Brad Smith, testifying in the same hearing, said the hack involved the work of "at least 1,000 engineers." While perhaps self-serving, these observations underscore a time frame and resourcing that are hugely impressive, almost as breathtaking as the fact that we failed to detect any of it while it was going on right under our noses.

General (Ret.) Keith Alexander, the CEO of IronNet, observed:

"I think the real objective is to gain information; they want insights into what's going on in our country. There have been no insights yet as to the Russians actually setting landmines as opposed to gathering information, but we can think of this as the recon phase. During this point of intrusion, they could set up backdoors so they have a way of getting in and out of the networks.

You don't necessarily have to set up landmines at that time; you would probably keep your information on those networks down low so that it's not detectable, and just have the backdoor capability to get in, and then do something when the need arises."

And so far, the apparent need has not yet arisen.

Eat The Software

A key step in the second stage was the compromise of Microsoft's Active Directory.

Gaining administrative control enables bad actors to pose as legitimate IT users, capturing the necessary authentication using valid credentials, and creating new, though bogus accounts, undetected. Threat actors are then free to move throughout an organization's IT systems posing as a legitimate user, alert-free. This, of course, presented a huge roadblock to detecting the bad actor once s/he was inside.

While the Active Directory hacks complicate detection, it's not an uncommon part of an advanced persistent threat. There is, however, one truly remarkable element that stands out within this attack, and that is the modification of the software build process.

Most APTs go after source code.

These guys got right into the compile stage, which is the last place anyone would look.

In part because no one would suspect that an attacker would embrace the "20 on a scale of 10" level of difficulty, and in part, because very few folks these days can read or write assembler code. Again, as Mandia has now warned, the implications of such a portable vector suggest many more breaches of this nature in the near term.

Theresa Payton, the former White House Chief Information Officer, opines, "This vulnerability allowed the nefarious cyber operatives to create what we refer to in the industry as 'God access or a God door,' basically giving them rights to do anything they want in stealth mode." Indeed.

Richard Clarke, the first U.S. "cyber czar" and current chairman of Good Harbor cybersecurity notes: "This is not just about an espionage attack. This is about something called preparation of the battlefield, where they are now able, in the time of crisis, to eat the software in thousands of U.S. companies."

"Most APTs go after source code. These guys got right into the compile stage."

This brings me to journalist David E. Sanger's observation that: "If a hacker went into your computer system just to read your email, that's pure espionage. But what people discovered over time, was that the same computer code that enabled them to break into somebody's system would also enable them to manipulate that system. … If the network was connected to an electric power grid, to a gas pipeline, to a water distribution system, to a nuclear centrifuge plant, you might be able to manipulate the data and cause havoc in those systems. And that's much more than mere espionage."

Is the recent activity at Oldsmar, Florida, where in early February, an (unknown) threat actor remotely accessed a computer for the water treatment system (using TeamViewer) and increased the amount of sodium hydroxide (a.k.a. lye) used to control acidity in the water, to 100 times the normal level … connected with the cyberattacks on SolarWinds, Microsoft and Accellion?

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

ICS/SCADA

Vulnerabilities

ICS/SCADA vulnerabilities climb into the billions these days as our connected IIoT Empire expands beyond simple math, leveraging the rich opportunity to accelerate the race toward digital transformation and, at the same time, likely presenting the greatest threat to the U.S. since, ever.

In fact, Accenture Security reports that "Indirect attacks against weak links in the supply chain now account for 40 percent of security breaches."

'Now,' as in, today, and not as in, tomorrow.

Drilling a bit deeper into the threat of IIoT devices controlling water systems, we find that of the approximately 54,000 drinking water systems in the U.S., almost all rely on some type of remote access to monitor and/or administer, most are unattended, underfunded and don't have 24/7 IT oversight.

A majority of these facilities, mirroring the majority of electric grid systems, have not separated operational technology (pumps, controls, switches and levers) from IT systems – inviting island hopping through an endpoint monitoring and control workaround. And, water systems present an attractive target because while the country can live without electricity for a while, the same thesis does not apply to drinking water.

We witnessed a water system attack back in 2013 when we saw bad actors breaking into systems that controlled the Bowman Dam in Rye, New York, and could have gotten access to its controls if it hadn't been offline at that moment for maintenance. Three years later, our DOJ charged an Iranian national with the attack, rationalizing that he worked for a company tied to the Iranian Revolutionary Guard Corps.

And in 2020, the Treasury Department sanctioned a Russian government institution accused of having created a destructive campaign called Triton, which targets public and private IIoT.

So the threats are very real, the next set of attack vectors have been nested in over 250,000 networks, including countless industrial control systems, and no one in the business of cybersecurity seems to know what to do about them.

> Fewer than 20% of risk professionals can identify a majority of their organization's IIoT devices … IIoT devices are typically attacked within 5 minutes of initial entry.

How Bad Is It?

A few eye-opening IIoT stats:

The 4th Industrial Revolution is poised to reach $1.1 trillion by 2026 (Fortune Business Insights), a breathtaking 24.7% CAGR.

The 4th Industrial revolution is poised to reach $1.1 trillion by 2026 (Fortune Business Insights), a breathtaking 24.7% CAGR.

IDC data estimates that 152,200 IIoT devices will be connected every minute by 2025. The math says that at this rate, by 2025, nearly 80 billion (79,996,320,000) devices are forecast to be connected annually.

Ericsson forecasts 3.5 billion cellular IoT/IIoT connections by 2023 due in part to 5G.

A Deloitte study reveals that digital transformation is a top strategic objective for 94% of executives, 85% have IoT/IIoT project budgets.

Ponemon, Symantec and Netscout report that fewer than 20% of risk professionals can identify a majority of their organization's IIoT devices, 75% of infected devices in IIoT attacks are routers, and IIoT devices are typically attacked within 5 minutes of initial entry.

And 55% of companies surveyed don't require third-party IIoT supply-chain provider security & privacy compliance.

The amazing thing about the law of large numbers can be most easily digested by examining the compounding effect of chess board moves. After the first move by both opponents, there are about 400 different board setups that may occur. After the second move, that number escalates to 197,000. After each player's third move, 120 million game variations will have occurred. After 4 moves, you get 10 to the 120th.

That would be 10 plus 120 trailing zeros. Almost twice the number of atoms in the observable universe. IIoT and 5G will drive our 4th Industrial Revolution, but they will also invite a second Cybersecurity Revolution.

One for which we are uniquely unprepared.

Cyber-Physical Systems

Cyber-physical systems (CPSs) are a new category of risk that include systems that orchestrate sensing, computation, control, networking and analytics to interact with the physical world (including humans).

They are the heart-beat of all connected devices where security spans both the cyber and physical worlds.

The open source TCP/IP stacks, which are used to manage most of these devices, impacted more than 150 vendors and millions of their products in healthcare during the last quarter.

IoMT (Internet of Medical Things) brings this concept into hyper-focus where it is easy to imagine pacemakers and defibrillators being attacked and their users and/or providers held hostage for ransom

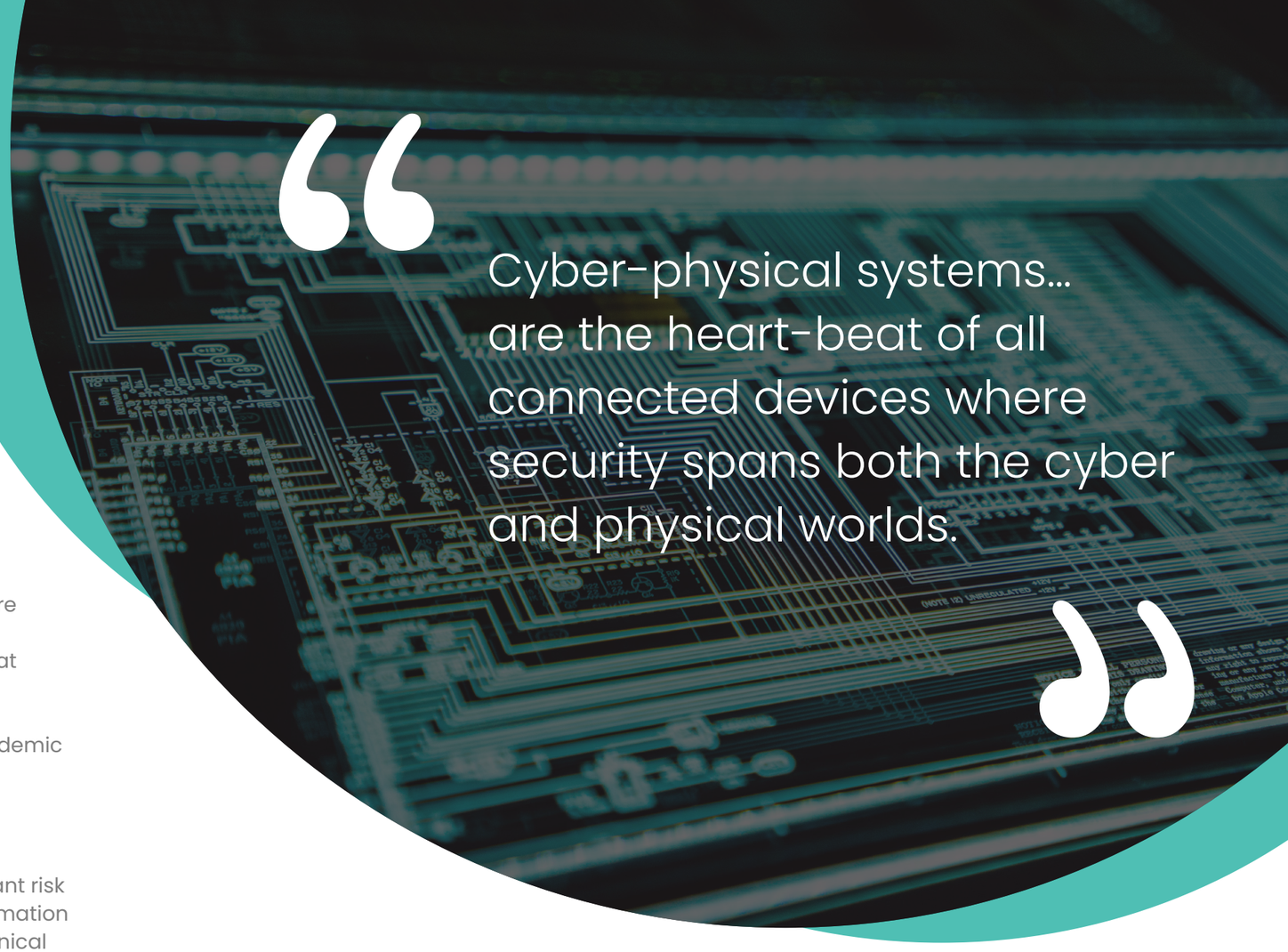
Attacks targeting IoMT and health information technology generally continue to grow and vulnerabilities related to the pandemic are amplifying the threat. At the same time, health systems have been rapidly growing their device inventory to meet the sudden surge in health care demands from COVID-19 and provide lifesaving treatment to those patients at grave risk.

Typically, because of the spinning pandemic clock, new IoMT, like those telehealth platforms, did not undergo more than a cursory security onboarding.

The result is an expanded and significant risk to patient safety, personal health information (PHI) confidentiality, and the overall clinical network.

Gartner predicts that the financial impact of CPS attacks resulting in fatal casualties will reach over $50 billion by 2023.

With OT, smart buildings, smart cities, connected cars and autonomous vehicles evolving, a focus on operational resilience needs an infusion of urgency. CISA and the FBI have already increased the details provided around threats to critical infrastructure-related systems.



Now, CEOs will no longer be able to plead ignorance or hide behind insurance policies.

Gartner predicts that by 2024, liability for cyber-physical security incidents will begin to pierce the corporate veil for CEO protection and hold CEOs and other C-suite leaders and Board members accountable.

And with this shift in liability laws, we may actually make some progress in getting to proper levels of cybersecurity defense and preparedness.

After a few disasters and massive wrongful death lawsuits, the C-suite may finally come to realize that this “security business” is actually their first priority.

Mirai Again.
Or, Still.

In addition to all of that exposure, on March 20th, the discovery of a new variant of Mirai was reported that leverages security flaws in D-Link, Netgear and SonicWall devices. Since early February, this variant has targeted six known vulnerabilities, along with three previously unknown ones, to infect systems and add them to a botnet network.

More than 60 variants of Mirai have been observed in the last 90 days and most of them take advantage of known or unknown vulnerabilities in IIoT devices. The latest attacks are based on a recent variant of Mirai's source code, targeting some additional, newly discovered vulnerabilities in IIoT devices across critical OT networks.

Six high alert CVE's had been issued months before the attack, yet no patches had been applied.

Russians Assert
Dominance

In the Ukraine in December 2015, the Russian Sandworm Team hacked into the Ukrainian power grid and took it down. The Russians gained access to the connected IT network, from which they pivoted to the SCADA portion of the network and manipulated the ICS controls to shut down power in Kiev.

This attribution is not speculation, Russia took credit publicly.

XENOTIME, and its association with the TRITON malware, is now the most dangerous IIoT threat actor, targeting a specific safety instrumented component within industrial control systems, designed to protect health and environmental safety in industrial settings.

Manipulated SIS (Safety Instrumented Systems)leads to loss of life. An SIS is designed to monitor dangerous conditions in a plant (operation unit) and take action in the event of a dangerous condition or a condition where if no action is taken it will cause danger.

The bar has now been raised.

Cybersecurity researchers are also convinced that Russian operators, like the Sandworm Team, have attacked and embedded malware in western ICS systems over the last few years, preparing for future attacks.

What are they waiting for? A really good reason.

Back To

The Future

Russian cyber operations represent a very real and current threat, and Russian intelligence services will continue to view corporations, governments and civil society as viable targets for espionage and disinformation operations.

Because it is working.

All of the campaigns discussed here have been active within just the past couple of months, and the pace with which these have progressed is unprecedented. These threats are not hypothetical.

Without a major shift in our defense philosophy, we will remain as sitting ducks.

We will need to work much more transparently with federal agencies upon the premise of collective defense, which will enable organizations to operate with visibility into threat intelligence, not only from their own networks but from the accumulated knowledge of multiple communities so as to discover active threats much more quickly.

And the question over what to do about them once discovered will find answers in the tenets of active defense, or dare I say it, offensive security.

Bringing this all together will require bold courage on the part of politicians and the private community, many of which will be naturally reluctant to share proprietary information, or work together without regard for private gain.

But that is what happens in war-time, and our political reluctance underscores the reality that it has been over 75 years since we have collectively faced an existential threat on a global scale, within the context of a world-wide threat to peace and safety.

The Next 90 Days

WHAT WILL WE SEE?

Not surprisingly, we should assume a continuation of the supply chain attacks, and an increase in both purse money and frequency of ransomware attacks leveraging the open doors left in the wake of the Exchange server attack flood.

We should also see a large scale ISC attack, perhaps not on U.S. soil but designed similarly to that of Petya/NotPetya, and released in the wild to test another self-directed attack of massive proportion.

We will likely continue the frustratingly slow progress we are making toward a public and private cybersecurity defense partnership, impacted by conflicting political agendas, internal squabbling, and hierarchical directives along with increased and emboldened rhetoric from both Russia and China.

Both countries will continue to flex their newly affirmed cybersuperiority with fresh global threats and expanded disruption.

Q2 will expose more point-solution competition from a collective of new players in the cybersecurity marketplace. Much of this competition will be fueled by large injections of venture capital into startups and early stage companies bringing AI and ML technologies to the automated detection and defense stage.

And we should see greater progress and competitive separation from Chinese dominance of the global quantum market with the first public announcement by a western nation of a quantum crypto break. At some point very soon, quantum computers will be able to demonstrate breaking the traditional public key crypto.

As tempting as it is to include increasing WFH threats as an easy prediction, I will simply suggest the obvious problems exacerbating from this continuing trend into Q2 will continue to increase in scope and complexity.

More Confusion,
Less Defense

As more people have adopted the work-from-home protocols, employees will take cybersecurity shortcuts for convenience, and insufficiently secured personal devices and routers, along with the transfer of sensitive information over unsecured or unsanctioned channels, will continue to serve as an accelerant for data breaches and leaks.

We will need, and might see, a stronger emphasis on detection of cybersecurity threats in Q2, as we all now know that protection alone has not defeated the biggest and most damaging cybersecurity threats in history.

Advanced, unified and extended detection and response vendors should see a majority of the spotlight in Q2 in concert with our first virtual RSAC. Visibility, detection and response, when it comes to threats characterized by unprecedented levels of sophistication, professionalism and maliciousness, will dominate the market.

We may also see an increase in the adoption of AI-based and machine learning Cloud SIEM tools, and an increase in automated threat hunting and orchestration in real-time, providing that more granular visibility so important to early threat detection.

Progress toward the 4th Industrial Revolution driven by the rise of 5G technology and new forms of IIoT connectivity, will provide more, not fewer, opportunities for cyber attackers to take over systems and networks. And popular mobile-only designs will intensify the inbound threat channels and stimulate the further elimination of perimeters while pushing increased cloud adoption, creating an additional extension of the threat landscape.

One that will become even more difficult to see and defend.

Trends & Gaps

Segregating unsecured IIoT and 5G-enabled devices from the rest of the network will be elevated to a common best practice in Q2, but fewer hygiene organizations will be able to comply, as the gap between trained and untrained cybersecurity personnel will continue
to widen.

Phishing will keep plaguing businesses in Q2 and the pandemic will remain a popular theme for psycho-intensive phishing campaigns, designed to lure information-deprived users with the announcement of a new vaccine, a shift in lockdown protocols or a surge in new infections. Embracing improved online education within a curated program for increased situational awareness may begin a trend toward a long overdue culture of cybersecurity readiness.

Fileless attacks and business process compromises will also increase. These threats are able to fly beneath the radar of conventional SIEM solutions and usually proceed undetected.

They will continue to do so.

This next quarter should begin an inflection point for edge computing. This of course, will further expand the attack surface and extend the opportunity for attackers to gain access through various entry points of the extended architecture. Businesses will generally not have insight into every device being connected to this extended network, and will thus create increased cybersecurity risks without understanding the threats imposed by the new topologies.

Containers, Kubernetes and micro-segmentation will all be rushed to adoption, resulting in increased pressure on the human factor to optimize configuration performance, at which we will fail at a greater rate than in the past.

Why?

Humans In The House

Because we have a prefrontal cortex.

It is the epicenter of our cognitive horsepower and delivers our ability to focus on the task at hand. Under normalized conditions, it runs on autopilot and we power right through mundane tasks. But in times of abnormal conditions and intense stress, our prefrontal cortex begins firing on cylinders it doesn't possess and causes us to focus on the step-by-step details of our performance, seeking an optimal outcome and, as a result, disrupting what would have otherwise been fluid and natural.

It translates to an increase in insider threat for which we are not prepared.

Unintentional insider threat will increase in Q2 owing largely to the gap in properly trained resources and the pressing need for every business to train and educate all employees in the fundamentals of cybersecurity risk associated with each emerging market trend.

These are the easy projections for next quarter, as they are largely a continuation of threat expansion from Q1, but there is more at work here than meets the eye.

Complicating the landscape are factors like increased complexity in compliance mandates and regulations, an increase in M&A activity resulting in the combination of cybersecurity threat defense capabilities without actual integration, and an increase in the general malaise and uncertainty about our abilities to compete on the battlefield.

So, the resulting market messaging will confuse and deflect while our adversaries continue to improve, educate and tool up, and we will continue to fall further back on progress in education and workforce development, on the discipline required of hygienic correctness, and on the recognition of the human factor's role in cybersecurity efficacy.

There is hope, and there is progress, but it's harder to find than in the past.

CYBER THEORY

cybertheory.io

212.518.1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018