Research Report

Third 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 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

Cybersecurity Landscape

Summary: Q3 2021.

In August of 2021, we saw fewer reported cyberattacks and data breaches, with only 84 incidents accounting for 60,865,828 breached records.

If not for the attack on T-Mobile, it would have been even smaller, affecting 53 million records and 7.8 million customers.

But the variety is astounding.

Everyone from Paxton Media Group to North Dakota's Sanford Health to Ibex, Vision for Hope, Chanel Korea and the Durham Region Children's Health Center reported incursions and successful breaches.

In lieu of revisiting the cyberattacks that occurred during July, August and September, it may be more useful to look at the emergence of the broader attack vector, which began to emerge in the first two quarters, pulling ransomware apart.

The trend our team sees now is the open-source supply chain and the frightening part is it looks much bigger in terms of scope and scale and much more difficult to identify, defend and stop in terms of complexity, depth and reach.

Dependency

Confusion.

Most cybersecurity folks were hoping the international attention earlier attacks on Colonial and JBS received would have frightened the cyber mob into hiding and reorganization, along with a resultant slowdown in the volume and nature of ransomware. Instead, we saw a side step to laboratory-grade supply chain attacks against the open-source ecosystem soar by 650% and a new vector class we call dependency confusion emerge, which is quickly becoming the overreaching attack technique of choice to close out the year.

And indeed, the former Eastern European gangs did take a momentary respite from savaging the Wild West. Our pesky friends at BlackMatter have just reemerged from DarkSide, the ransomware-as-a-service best known for the takedown of Colonial Pipeline.

Another gang whom we know as REvil had also been on staycation since its wildly successful attack on Kaseya, but we now see a completely refreshed online presence with new servers and a new list of victims.

None of these dark web maneuvers matter, as what's important is the development of supply chain attacks against the open-source ecosystem and its soon-to-emerge dominance over all other attack vectors.

Some will call them sophisticated because instead of waiting for vulnerability disclosures, attackers are proactively injecting new vulnerabilities into open-source projects that feed the global supply chain and then exploiting the vulnerabilities they've created.

Sophisticated or

Just Lazy?

We will spare you our rant on open source in the most vulnerable attack landscapes, but the short-form version is: We have a problem.

Sonatype, a DevSecOps automation specialist, found that nearly 3 in 10 of the most popular Java, JavaScript, Python, and .NET projects contain at least one known security vulnerability. The challenge is that

popular open-source projects have more known vulnerabilities overall, and developers using them are also less likely to be stuck in a situation where there is a known vulnerability but no remediation path.

But the reality implies that to stay in control and continue to support business initiatives, disciplined dev teams need to actively manage these dependencies and ensure they are moving to newer and non-vulnerable versions in a continuous manner.

Who does that?

Almost no one.

While development teams believe they are doing a good job fixing defective components and think they understand where risk resides, the objective data tells

a different story. In fact, the data says they make suboptimal decisions 69% of the time when updating third-party dependencies.

7/10 is a big number.

Think about your own dev teams; then let's talk open source some more.

Objectively, the research shows that most development teams are not following structured guidance with regard to dependency management and, as a result, they are not actively remediating known risk within their software supply chains.

Instead of waiting for OpenSSF or the Consortium for Information and Software Quality, we would recommend standing up a quality check and SBM initiative to prove that our internal team was working with maximized cleanliness and hygiene from the start.

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

The Pivotal Question.

The pivotal question is: Does the rush to digitization and the fourth industrial revolution justify the exposure and vulnerability and the expanded threat landscape we are bringing upon ourselves?

Process automation seems like a logical choice, yet when we consider GitHub's recently identified high-severity vulnerabilities in Node.js packages alone, which could be easily exploited to achieve arbitrary code execution, we realize we are expanding complexity rather than reducing it. And as we assess success with SOAR, are we convinced we have the level of automated intelligence equal to the task?

The last nine months have revealed several high-profile software supply chain attacks, including the SolarWinds hack that affected several U.S. government agencies, Microsoft and FireEye, among other organizations, and the ransomware attack that encrypted the data of more than 1,000 Kaseya VSA customers.

Those are facts.

Instead of making progress against the growing tide of incoming cyberattacks, it seems we set the table each month with new vulnerabilities and easier access paths, in effect, joining forces with our adversaries by easing access to our crown jewels. In our research, these efforts also get almost no media coverage, and are seemingly in the same bucket as other international events that can't be easily explained. As a result, many in our industry wake up surprised at the increase in access points created almost magically overnight.

Is it that we cannot admit, acknowledge and accept that we are not up to doing the required foundational hygienic work required in cybersecurity, or is it that we lack the leadership smarts to recognize that not all

organizations are prepared for agile development and DevSecOps deployment and that we also fail to recognize the dangers?

If we continue along the trail we have forged in the first three quarters of 2021, our near-term destiny will continue to be earmarked by battlefield failure, most of which will be sadly self-inflicted.

The Risk Threshold.

To illustrate the threat and risk threshold, consider the state of today's open-source supply, demand and security dynamics:

Supply has increased by 20% YOY. The top four open-source ecosystems now contain a combined 37,451,682 different versions of components.

Demand has followed and increased by 73% YOY. In 2021, it is estimated that global developers will download more than 2.2 trillion open-source packages from the top four ecosystems. Despite the growing volume of downloads, the percentage of available components utilized in production applications is shockingly low.

We found projects with a faster mean time to update (MTTU) to be more secured, yet by a tiny factor of only 1.8 times less likely to contain vulnerabilities. We also saw that popularity is not a good predictor of security.

The most popular open-source projects were three times more likely to contain vulnerabilities.

How the Open-Source Supply Chain Operates.

A supply chain attack's objective is to infiltrate and disrupt the computer systems of a company's supply chain in order to harm that target company.

The premise is that key suppliers or vendors of a company may be more vulnerable to attack than the primary target, making them weak links in the target's overall network.

For example, the Target attack through Fazio Mechanical Services, its third-party vendor providing heating and air conditioning services, carelessly allowed the bad guys to steal its network credentials and thus obtain admin access to its ERP system. Small company, weak security systems, and lack of awareness.

Supply chain attacks expose a conundrum in a company's supply network that discloses that an organization's cybersecurity controls are only as strong as those of the weakest party on the chain. Because of its development process, open source follows a chain of contributors and dependencies before it ultimately reaches its end users. It is important that those responsible for their user or organization's security are able to understand and verify the security of this dependency supply chain, yet therein lies the rub.

Almost all companies dependent on open-source supply chain do not audit nor do they understand the exposures and vulnerabilities inherent in the software.

In an attempt to reverse the cycle and shore up the unknowns from the knowns, OpenSSF, a cross-industry collaboration, brings together technology leaders to improve the security of OSS by creating a future where participants in the open-source ecosystem use and share high-quality software, with security handled proactively, by default, and as a matter of course.

Unfortunately, its work to date on the problem has demonstrated no progress of note.

As is the case with similar projects, the bulk of the strategy rests on hope, and in this case, will run out of time before any positive impact can be realized.

Another organization working to address the challenge is the Consortium for Information and Software Quality, a special interest group under the technology standards body Object Management Group. One of the standards the organization is working on is the software equivalent of a bill of materials. It will let enterprise customers know the components that go into the software they're using, and if any of those components have known security problems.

Microsoft is involved, as is the Linux Foundation and other big players, adding up to about 30 companies total.

It's a valiant effort, but if you are in the field with supply chain relationships, you will have to do your own work.

Refresh.

Reminder that any company that produces software or hardware for other organizations is a potential target of attackers. Nation-state actors have deep resources and the skills to penetrate even the most security-conscious firms.

Security vendors can be juicy targets. In the case of SolarWinds, for example, one of the higher-profile companies breached was FireEye, a cybersecurity vendor. FireEye says that the attackers didn't get into customer-facing systems, just the penetration tools used for security testing. Mimecast, Microsoft and Malwarebytes quickly joined that list.

The fact that any of these got hit at all is worrisome.

It demonstrates that any vendor is vulnerable and could be compromised. In fact, this fall, security vendor ImmuniWeb reported that 97% of the world's top 400 cybersecurity companies had data leaks or other security incidents exposed on the dark web, and 91 companies had exploitable website security vulnerabilities.

But this new focus on open source is the most worrisome of all. Today, the proliferation of open-source vulnerabilities make it impossibly irresistible. In addition to the JPD (just plain dumb) threat, folks like China have been compromising U.S. military, government and critical civilian platforms for years so that intentionally folding a Chinese supplier into our supply chains is essentially suicidal. In spite of that, nearly every government organization and private company is exposed, to some degree, to technology that originates in China or other low-cost supplier countries.

"In fact, this fall, security vendor ImmuniWeb reported that 97% of the world's top 400 cybersecurity companies had data leaks or other security incidents exposed on the dark web, and 91 companies had exploitable website security vulnerabilities."

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

What Can We Do?

If we are still committed to plowing ahead with business-driven digitalization initiatives, there are a few things that we can turn to for some level of support. Regulatory frameworks, in the financial sector or healthcare, already provide for third-party risk testing or have some standards that vendors need to comply with, as within PCI, there's a software quality component to test the quality of mobile payment components.

The Capability Maturity Model (CMM), ISO 9001, Common Criteria, SOC 2 and FIPS-140 all should become part of audit criteria, regardless of cost and inconvenience.

If we start demanding more testing, or regulators step in and mandate better controls, then the costs of these audits are likely to drop and we will also see more innovation, such as bringing us back to the beginning in automated testing and orchestration.

We actually have effective AI/ML technologies that could take over these processes, but it may be that we are moving so fast, potential solution vendors are not even seeing the opportunities therein.

In our upcoming launch of CyberEd.io, we have dedicated a lot of lifting to the issues around DevSecOps and open-source supply chain exposures, and it is our intent to keep the spotlight focused on this threat vector until we close the gap between the traps and the designs.

It can be done.

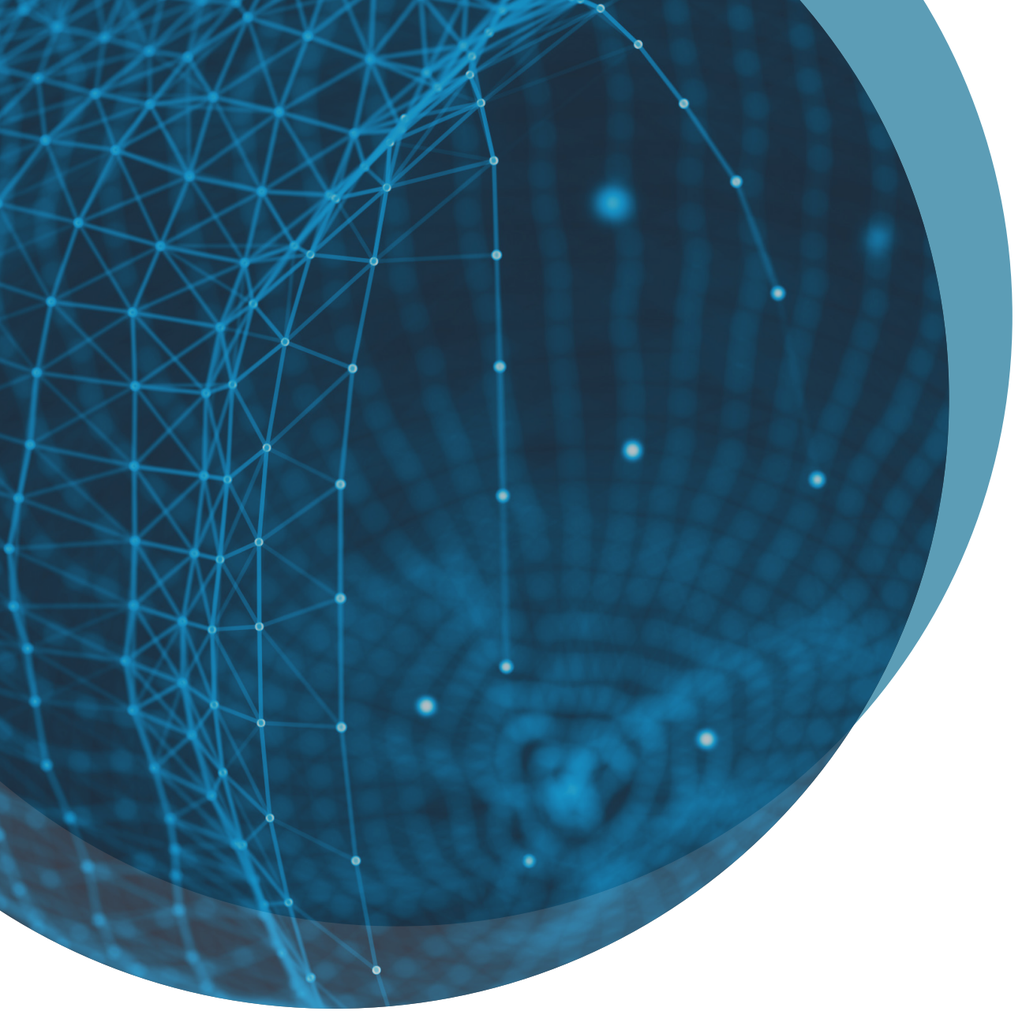
Levi Strauss for example, vets its software vendors today by requiring them to have demonstrable, auditable proof that they have implemented a security framework and can demonstrate compliance with that framework, while taking a dim view of leveraging open-source supply chain options.

It is all a function of your risk appetite and understanding your capabilities in context. JPMS will have a different view of each than a Levi Strauss.

Software works the way it works. There is no galaxy where on Mars software works one way and on Venus, it works another. This should represent a huge advantage to folks trying to defend against incoming threats, but the problem is in the ecosystem, the complexity and the way it's put together.

We are proponents of Zero Trust and firmly believe that an organized campaign that starts with the identification of critical assets and the establishment of a small protect surface around those assets through network microsegmentation and strict least privilege with continual MFA, and limiting Internet-facing software to minimal web access permissions, is the pathway toward resetting your existing network within that ZT context over time.

Whatever we do, it needs to be different than what we have done, or we will have no chance against these adversaries.



Cyber-Physical Systems

Become the Tail That Wags.

Cyber-physical systems (CPSs) remain in the news (Colonial and JBS) as the vulnerabilities continue to surface as essentially becoming unmanageable in a cyberthreat context

They are the heartbeat of all connected devices where security spans both the cyber and physical worlds, and combined with open-source supply chain threats, they will soon become world-shaking targets of attacks.

The open-source TCP/IP stacks that are used to manage most of these devices continue to expose hundreds of vendors and millions of their products in healthcare, manufacturing, pharmaceuticals, critical infrastructure across energy, electrical, oil & gas and water systems and other lesser segments during the first three quarters of the year.

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 for hostage.

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.

And we now know that COVID-19 is one variant of many and that isolation, masking and vaccination may become our new realities, or they may not.

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.

One Significant Event.

The follow-on momentum from Biden's executive order signed in May, which outlines several cybersecurity measures and requirements intended to harden our nation's digital infrastructure, will impact our world in several significant ways.

One is a real timeline toward federal agencies adopting Zero Trust architecture.

Most security protocols assume that if you have the credentials to access a certain network, you can be trusted to work in it. Zero Trust removes that assumption with continual multifactor authentication and more expansive data encryption, microsegmentation, protect surfaces and a focus on data, access, applications and services.

Within 60, 90, and 180 days of the order being issued, agencies will be required to first, update their existing plans to adopt cloud technology and second, to work with the Department of Homeland Security and the General Services Administration to develop and issue cloud-based security standards.

While the order addresses seven core areas, sections on software supply chain security and threat information sharing requirements within one year are most likely to have an impact on businesses.

Organizations may not realize they are bound by the order – even if they aren't a federal contractor.

And finally, there is the requirement to actually adopt and implement some of the Zero Trust architecture described above.

The SBOM (Software Bill of Materials) is in there, and while it would not have helped in the SolarWinds fiasco, it will help our DevSecOps teams better prepare for open-source supply chain attacks. Similar to FDA requirements for medical devices such as pacemakers, SBOM requirements are expected to mandate that organizations list all the components used in their software, including libraries, drivers, firmware, licenses and operating systems. The order also requires that organizations secure their software development processes and access controls.

To Whom Will It Apply?

Essentially everyone, as your software development company is likely to be part of the federal government software supply chain even if you don't know it. By extension, any vendors whose products are used by those developers — hardware providers, for example — are part of the chain.

Besides direct federal contractors, the order also applies to broad commercial subsectors. Companies that supply to defense contractors (or whose software or hardware end up in a contractor's products or services) are in the supply chain and in a position to introduce risk.

Additionally, it is expected that the National Institute of Standards and Technology will publish supply chain security standards that will likely become a security industry standard. Software and hardware suppliers to state and local government and private sector entities should expect changes to become compliance requirements in the future.

A Word or Two About
These Markets.

Many cybersecurity marketers have fallen for the lure of tying their product or service to Zero Trust as though, by simply doing, they will elevate beyond the wall of noise and into the hearts of their prospects.

Not only has that not happened, but the opposite is true.

The last decade is gone. The new decade looks as different from the last as a Tesla does to a 1956 Buick. And in every way.

Instead of four or five true competitors, marketers now find themselves staring at 20-25 alleged competitors, all saying essentially the same thing as each other. CISOs have gone from polite, available to all, denizens of a commercial threat protection landscape to isolated, impossible to reach, and grouchy recipients of sales and marketing pitches, if you are lucky enough to contact one directly.

The wall of noise is high and thick, and no one believes that everyone can lead you to the Zero Trust Promised Land.

The problem from our point of view is that most marketers have approached this near-impossible state with the exact same tools and perhaps mentalities they were using to penetrate the prior markets, which may have worked then, but will surely not work now.

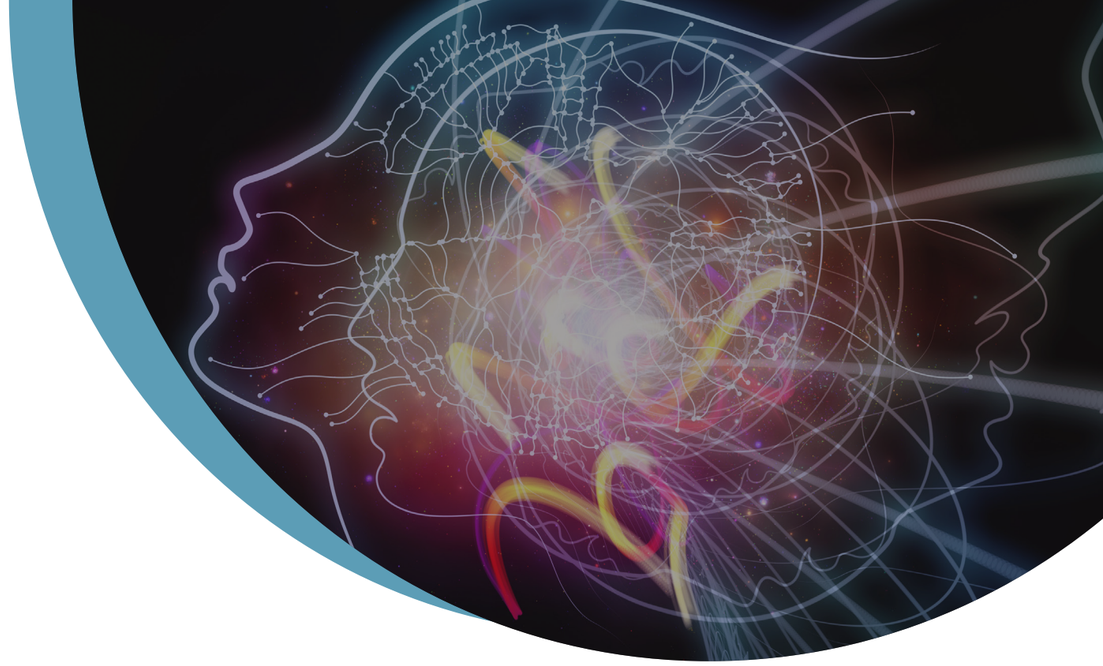
Every CISO we know has been to a dozen Virtual Roundtables – no one has not figured out at least five ways to accommodate the "new" (now 18 months old) work from home environment. No one we know wants the 2021 Cybersecurity Awareness Month Resource Kit and absolutely no one wants to know what can be done to predict or prevent an incident like SolarWinds, Accellion, Codecov, and Kaseya from happening in the future.

If they are all doing their jobs, none of this is relevant. If they are not all doing their jobs, why do you want them as prospects? They will have smaller budgets, more bureaucracy, less focus and a suboptimal understanding of their condition.

The CAC for these folks is very high and the ARR will be very low – in fact, it is likely you will have increased churn as these personas will have little or no idea how to extract value from your product or service, post-install.

This is not a how-to tutorial, but rather a directional beacon in a storm.

What you as vendor marketers need to do



today is focus on who you are, how you do what you do, a mapping of that process to the industry's most popular trend, and the most unique and credible way to deliver that message.

In journalism, there are myriad rules that govern professional reporting. This is why we rarely see deeper dives into main or substory lines that take us to a place that actually makes us think about a problem.

If we told you that we were hosting a discussion with Joe Lock, the CISO at GrowRich and an industry expert from the money management business on personal finance care in an age of cyberthreats, and at the same time, you received an invite to a fireside chat with Chris Bosh on his views of technology in the workplace, which would you attend?

If our invite had Art Coviello on the current and future threat landscape, and another had anyone else, which would you attend?

If the godmother of SAML and UMA sat down with one of your SMEs to discuss the first- and last-mile challenges of decentralized identity, would your prospect audience be more or less inclined to choose that over your invite to the webinar on how the Chief Security Officer should work with the Chief Privacy Officer, by a vendor CISO?

How about instead of $200K spent on 1%-2% conversion rate content syndication campaign leads, you spent it on lighting up the sky over Orlando at this fall's Gartner Security & Risk Management Summit with 300 drones dancing out your brand story and tying your solution indelibly in prospects' minds to Infrastructure Protection Strategies.

Bottom line?

You need to do more than you are doing.

And you need to do it differently.

A Late Entry

Before we close the 3Q chapter, we would be remiss in failing to mention the Sept. 20 supply chain attack on NEW Coop, the farmers' feed and grain cooperative with over 60 locations throughout Iowa.

Demonstrating just how deeply and broadly the U.S. economy and our supply chains are interconnected, our BlackMatter friends just dealt a ransomware attack to this network that supplies 40% of US grain production and 11 million animals' feed schedules. They're now demanding $5.9 million in exchange for a decryptor and a promise to not leak stolen data.

What was seized included 1,000 gigabytes worth of files, including invoices, research and development documents and the source code to the company's soil-mapping technology.

BlackMatter, as you may recall, was one of the gangs that promised it would not target "Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities)."

Now, with $6 million hanging in the balance, NEW Coop begged BlackMatter for an explanation, given that they think of themselves as critical infrastructure, and that the attack will lead to food supply disruption for grain, pork and chicken.

NEW went further to plead with BlackMatter, "I am just telling you this so you are not surprised as it does not seem like you understood who we are and what role our company plays in the food supply chain."

This one is worth watching as it can potentially set the direction for a bunch of weather vanes.

The Next Quarter.

As we have pointed out, exploitation of the open-source supply chain will accelerate a continuation of these supply chain/ ransomware attacks, and an increase in both fiscal demands and frequency.

We should prepare for a large-scale Industrial Control attack, 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 union, 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 cyber superiority with fresh global threats and expanded disruption.

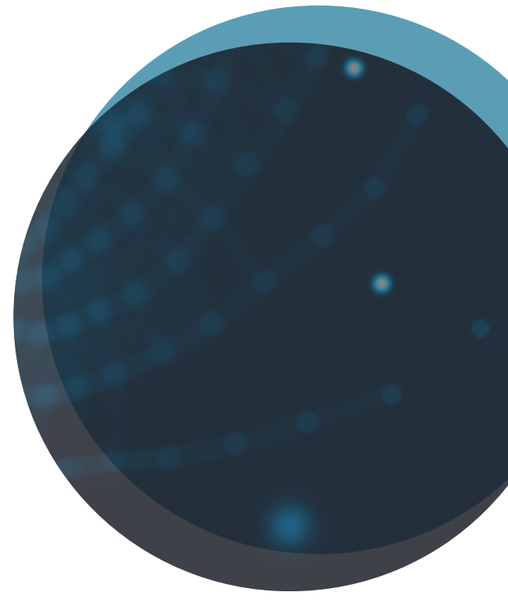
Q4 will expose more point-solution competition from a collective of new players in the cybersecurity marketplace. Much of this competition will be fueled by large injections of venture capital into startups and early-stage companies bringing AI and ML technologies to the automated detection and defense stage.

$45 million series B rounds had been unheard of, even in the heady days of 2020, yet they have become commonplace today. $250 million investments in spinoffs like VisibleRisk to BitSight by Moody's and Team8, position incomplete, though popular board-level solutions as front-runners in the race for huge-value IPOs or acquisition.

Another quarter will bring 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.

WFH and borderless perimeter threats will continue to reveal new problems exacerbating a continuing trend into Q4, like the data coming out of every study about the reliability and dependability of VPNs.

More discovery will continue to showcase an increase in scope and complexity.



Lots of Confusion.

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 Q4, 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 Q4 in concert with another 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.

Or we may remain so busy fighting off big, incoming threats that we won't have time to address and/or properly assess any new technologies, regardless of promise.

As Mark Twain said, "The future interests me, as I am going to spend the rest of my life there."

Indeed.

CYBER THEORY

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