United States House of Representatives

Homeland Security Committee – Subcommittee on Cybersecurity and Infrastructure Protection

Testimony of Mr. Joe Head – Co Founder and Chief Technology Officer, Intrusion, Inc.

Good morning, and thank you Chairman Garbarino, Ranking Member Swalwell, and distinguished members of the subcommittee. My name is Joe Head. I am the cofounder and Chief Technology Officer of Intrusion – proudly headquartered in Plano Texas.

It is both a privilege and an honor for me to be here today, sharing my technical expertise and insights, which I have accumulated over four decades of immersion in the cutting-edge realms of the cybersecurity industry. I wholeheartedly commend the dedicated individuals on this subcommittee and their staff for their tireless efforts. They understand the need to enhance the Federal Government's cybersecurity capabilities but are also channeling their energies toward advancing the mission of agencies like CISA, with a strong focus on developing next-generation software and technologies that are critical in the forthcoming cyber conflicts.

I began designing and providing secure networks and other security solutions for the US Government when Ronald Reagan was President. We built equipment for the hot line from the White House to the Kremlin during his second term. I co-founded my company Intrusion in 1983, just 3 years out of college and we've been a public company since the 90's.

I've had more fun designing and securing things than you should get paid for. My goal today is to help the committee spur innovation in security. The US is not secure. There are some secure networks, but very, very few. Complacency with the state of our security is a serious risk. A relaxed defender is the most naïve one. Cyber offense is winning everywhere. A great challenge of our time is to make defenders better able to defend. I have an old friend who liked to say that he'd rather be lucky than smart. A network or system not breached is not a matter of the defender being lucky or smart, it is sadly that an attacker just isn't interested enough to focus on breaching it.

As you read my opening remarks, keep in mind that an outline of the Manhattan Project was not put in the Congressional Record before Los Alamos was built. Our government needs people with technical depth and a winning mindset. My job is not to inform our enemies what we plan to do to win the cyber war but to methodically ensure we take this domain. We do know what to do. There are core experts both in government and industry that understand what winning would require and how to get there. This path also includes how not to get there by spending billions unwisely.

Today I too often see security plans and programs looking a lot like children's soccer – a bunch of kids clustered around the ball. In cyber, the kids are always automating the hottest buzzwords without a grand plan to produce an absolute win. The challenge is to wisely architect a plan, put the right people in charge of defining the requirements, manage a design production, and reliably deploy a cyber get-well plan.

We must have a get-well plan in cyber which gets silently built and deployed, representing a master stroke in reversing the reality of our current predicament. Adversaries all over the world are killing it in cyber with massive asymmetry, winning and penetrating millions of systems that we need to be trustworthy. Many are capable hackers working inside adversary cyber operations or just as individuals on their own.

It was in the 1990's while identifying a threat at an automotive manufacturer that I realized we needed a better way to find the needle in the haystack. I built a database to understand what the Internet looks like, who owns what, which areas were unsafe to visit. This analytic engine has evolved into a mainstay of defense in depth cybersecurity. By the early 2000's we built a tool to inspect and audit Internet travels. Today, we know what traffic is coming and going from monitored systems, but more importantly how to stop threats from impacting operations.

Now is a critical time for the US Government, US critical infrastructure, and critical parts of US industry. If the world was awesome at cyber security, there wouldn't be a breach every 37 seconds. The more you know, the worse it looks. Is it hopeless, no. Is there reason to believe that the USG will naturally solve the problem, no. But the entirety of the nation faces continuous and advancing attacks precisely because of US commercial and governmental successes, so the USG must strategically cultivate protections.

As a student of history, we have seen dramatic examples of innovation in the face of new threats. There were dramatic examples in WW2 when foreign threats and war drove US innovation to new heights. Sadly, few programs in the cyber field are constructed to be game changers. Mostly they scale up and automate a few elements of a good security approach but are not master strokes of a comprehensive solution. In other words, when the projects are done you won't be truly secure. Well-automated partial solutions don't make you secure, they just delay risk and make companies poorer from the expenses. While we must improve our baseline defensive posture to exponentially increase the cost of attack, profit motivated hackers, criminals, and adversaries have already doubled-down on their attack investments with extensive resourcing.

We already know that signature-based defenses fall in the face of zero-days and basic offensive threats. Most defenses ignore attacks via trusted sources like supply chains and security tools. The adversary is operating faster than the decision cycle of defenders, hidden in the vast noise of network traffic. Similarly, most budget requests and coding projects are to scale up defenses that cannot see novel compromises that have never been seen before, much less stop these threats completely. We have the capability now to tell if the crown jewels leave on a path headed for the shadows. With the advent of machine learning, network tools have identified and blocked untrustworthy sites, automatically guiding both people and devices to avoid the untamed internet, or offering them a picture of the monster rather than letting them directly reach out and touch it. But the unknowns must also be stopped, which requires knowing what good looks like.

Enemies are already exacting heavy costs on the US with cyber. Threats have been quietly planted into our infrastructure. Today – our country is still too reliant on foreign factories and vulnerable supply chains. The US does not make the computers, routers, switches, process controllers, dock cranes, pumps for gasoline, car parts, cameras, medicines, chemicals, and many other electronic things. But in cyber, it is much worse if your adversary made all the computers used in critical infrastructure or weapons systems. If your enemy left a back door or a designed-in a kill switch - they might use it. True security requires covering the supply chain threat as well as all other classes of threats like hackers and the insider threat.

Solutions

Why was I interested in testifying on this topic today? I believe that there is a chance that the US can re-achieve the needed sense of urgency these threats require. Investments in critical infrastructure, strengthening supply chains, and reshoring critical manufacturing are all necessary investments for our security. We must continue to be proactive in our approach to cybersecurity.

The allocation of over $400 million in funding for the transition from Einstein to CADS is a significant level of funding. It is imperative, however, that the CADS program design and implementation are meticulously executed to deliver not only enterprise-wide system monitoring and control but also the seamless handling of vast volumes of data and information. Intelligent and actionable outputs must be quickly and proficiently delivered to a broad audience. History has shown that well-intentioned technological advancements can be hindered by overly complex and convoluted designs, drowning users in a sea of tools and unnecessary complexity. We must keep in mind that offensive cyber operations can be cheap and flexible. Just like water can find any hole in a ship, building, or computer system and cause massive damage – a cyber attacker needs only to be creative enough to find or create one hole to get in and defeat you with cyber. We must remove those attacks from the shadows of the Internet, cut through that barrage of noise, and enable network defenders and analysts to discover the anomalies in the trusted high ground, where the maturing US cyber workforce can collaborate to investigate without having resources overwhelmed. We can start by identifying what good looks like. How should safe software and devices behave? Knowing these profiles drives proficient identification of threats.

Concurrently, we must remain vigilant against the pitfalls of comprehensive coverage leading to comprehensive failure. Adversaries will monitor our progress and respond. In the realms of design, application, and deployment, we must consistently ask ourselves how to intelligently and efficiently innovate new capabilities and approaches into a far more effective solution. This ensures that our legacy solutions, designed to address legacy problems on a massive scale, are agile enough to perform effectively in real-world scenarios.

To achieve success, systems like CADS must work quickly, easily, and reliably. That is difficult. Solutions need to respond immediately to a threat, preventing outbound communications and impact to system operations. The response should be simple and as automated as possible – and not labor intensive – overwhelming our already-taxed defenders. Plans need to account for integration and sustainment at the outset. And be agile enough to know that new things will need to be included over time. Our systems need to be real-time, 24/7 without a nagging string of alerts. A system that is both powered by quality and comprehensive data.

Beyond the outside threats, the CADS system should support zero-trust principles to mitigate and uncover compromises of accounts and systems. Digitally this means understanding the following about a system and its users:

- Who are the users?
- How do they behave?
- What is their reputation?
- Who have they been associating with?
- What does normal activity look like for mission need?
- What are the indicators of malicious intent?
- What are common traits of targets for a particular attack?
- How can targets reduce their exposure before being targeted?

Moreover, it's essential to examine how a relatively modest investment in pioneering technologies and capabilities could potentially revolutionize our cybersecurity approach. By allocating funding to these "moonshot" endeavors, even in the order of a few million dollars, we may uncover the next major breakthrough in cyber defense, at a cost that pales in comparison to the budget required for comprehensive systems like CADS.

We strongly recommend these flagship programs and agencies acknowledge that without specific and targeted funding for strategic research and development, we run the risk of neglecting the cyber defenses necessary for the latter half of the 21st century. DOD does this with DARPA and other programs. That’s one model, but any substantial investment in major cyber defense programs, without accompanying funding for innovative and transformative technologies, could render these programs vulnerable. Much like the Maginot Line, an unforeseen breach in an inadequately defended area could undermine the entire defense system, rendering it futile and ineffective.

As I conclude my opening remarks, I would like to emphasize to the committee that while the introduction of the CADS system seems to represent a significant stride in the right direction, we must not let complacency take root. We should actively seek ways to complement the capabilities of CADS with innovative functions and useable systems that align with our overarching mission of fortifying the US cyber defense posture. By doing so, we can ensure that our nation remains at the forefront of cybersecurity, prepared to confront the evolving challenges of the digital age.

Just like the Manhattan Project would not have worked without a core team of geniuses backed up with a massive support and implementation program – now is as good a time as any to take charge. Congress can wisely pass laws and fund efforts that guide the course of this cyber conflict. We don’t need to wait for our communications, power, logistics, and critical infrastructure to be taken offline in the lead up to a conflict.

Spending tens of billions on the latest partial buzzwords isn’t a winning strategy, let’s implement a winning cyber strategy on a tight timeline at an achievable budget. This path doesn’t stop the kids’ soccer teams from doing what kids do with massive pieces of federal budgets, so let’s carve out 5% for a cyber Manhattan Project that surprises the world with a defensive cyber solution that came out of nowhere and reversed the asymmetry of this conflict which we are losing. Winning is better.

Thank you again Mr. Chairman and Mr. Ranking Member for inviting me into this subcommittee’s discussion today. I would be happy to answer your questions.