SENATE SELECT COMMITTEE ON INTELLIGENCE

Robert Sheldon
Director, Public Policy & Strategy
CrowdStrike

Testimony on Protecting American Innovation
Industry, Academia, and the National Counterintelligence and Security Center

September 21, 2022

Chairman Warner, Vice Chairman Rubio, Members of the Committee, thank you for the opportunity to testify today. Innovation is an essential theme of the American story, so much so that the Constitution even includes a clause intended to protect it.[1] While the private sector is not the sole source of innovation in the country, it plays the leading role in actualizing new innovations from everywhere. This includes bringing to market developments based on the aggregate work of government, nongovernmental, and academic and research institutions. When the best innovations can reach scale, all Americans stand to benefit, in addition to many others around the world.

The private sector is incredibly diverse. When explaining CrowdStrike perspectives to stakeholders in the policy community, I am proud to mention that we protect 15 of the top 20 U.S. Banks, 69 of the Fortune 100 companies, and a significant and growing portion of the U.S. ".gov." But given the nature of the hearing today, I also want to emphasize that we proudly protect organizations of all shapes and sizes. We protect small, family-owned agricultural enterprises. We protect advocacy organizations for persecuted ethnic minorities abroad. We protect important nodes in domestic manufacturing supply chains. And we protect small start-ups commercializing cutting-edge research and development (R&D).

Like markets themselves, threats to the private sector are dynamic. Threats like theft, extortion, harassment and coercion, destruction, and espionage date back centuries or millennia. Analog versions of these threats exist today, but the advent of the cyber domain has changed their scope, scale, and impact. Over the past two decades, industry has faced an increasing onslaught of cyber exploitation and attack. All too often, these threats have devastating consequences for families, communities, and the economy. Particularly in the aggregate, these consequences extend to national security.

This hearing, and the Committee report that catalyzed it, are particularly timely. The private sector today differs materially from previous decades and the threat environment evolves with each passing year. As underlying conditions change, it's appropriate to periodically evaluate the array of institutions meant to protect industry, the services they offer, and in turn the basic expectations policymakers might place on elements of industry. I'm honored to share some

[1] Article I Section 8, Clause 8 (informally called the "Patent and Copyright Clause").

insights from our work across government and industry and identify some areas where we as a nation can strengthen security outcomes.

Overview of the Threat Environment

Today, the private sector faces a diverse and high-volume array of cyber threats. CrowdStrike research published this month identified campaigns targeting 37 distinct industries and a 50% increase in interactive intrusions over last year.[2] Regarding nation-state threats specifically,[3] numerous countries have developed cyber operations capabilities and routinely target U.S. industry. China (PANDAS), Russia (BEARS), Iran (KITTENS), and North Korea (CHOLLIMAS) represent the most potent threats.[4] These include:

Espionage. Cyber threat actors persistently spy on private industry. In some instances, they seek to steal intellectual property, later providing it to state-owned entities or national champions. In other instances, espionage targets sensitive business information, which can be leveraged to manipulate markets (e.g., by subverting bidding processes), understand corporate plans or strategies, or otherwise gain an unfair competitive advantage.

Theft. Cyber threat actors sometimes directly steal resources, typically currency or digital assets. These attacks can be sophisticated, compromising significant banking or payments infrastructure, or unsophisticated, and target poorly-defended individual accounts. A common form of attack is Business Email Compromise (BEC), where threat actors impersonate executives, hack and alter payment data, create fake invoices, or otherwise persuade finance personnel to make unauthorized payments. While eCrime actors conduct these types of attacks, so too do some nation state actors seeking to raise funds for government or military endeavors.

Extortion and coercion. Many attacks seek to extort victims for funds or other concessions. This includes ransomware campaigns or leaking or threatening to leak hacked data. These attacks can halt or severely degrade business operations and adversely affect corporate brand and reputation. Attacks like social media account takeovers and web defacements are more commonly associated with "hacktivist" actors than nation-states, but these techniques can be used for coercive effects.

Disruption and destruction. Relatedly, hackers can disrupt or destroy Information Technology (IT) and/or Operational Technology (OT) environments with wiper campaigns (which erase data

---

[2] *See generally, Falcon OverWatch Threat Hunting Report*, CrowdStrike (Sept. 2022), https://www.crowdstrike.com/resources/reports/overwatch-threat-hunting-report/.

[3] CrowdStrike tracks actors according to motivation, and typically classifies them as nation-state actors, eCrime actors, and "hacktivist" actors. At the Committee's request, I've focused my remarks on nation-state actors, but will briefly describe eCrime overlaps and use of more traditionally 'hacktivist' themes or techniques.

[4] *See* George Kurtz, *Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence (Feb. 23, 2021 at 3)(Quick overview of CrowdStrike's threat actor naming conventions), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf.

including potentially that required to make devices function) and encryption (e.g., ransomware or pseudo-ransomware).

Subversion. In some instances, companies are attacked or their infrastructure subverted simply to attack other public or private sector entities. These supply chain attacks can be extremely targeted, affecting a single or small handful of victims, or can effectuate compromise of thousands or tens of thousands of victims.

Adjacent threats. Three additional types of threats with a nexus to cybersecurity are worth mentioning here. First, under the guise of security, some countries have formal or informal code-review requirements, requirements to provide encryption or other security-related data, forced technology transfer requirements, and/or excessive "lawful access" requirements. These threats are a form of mandated vulnerability by coercion, and they are most acute in countries with weak or nonexistent rule of law. The People's Republic of China leads the field in these areas, but other countries are following suit. Second, insider threat attacks can be analog in nature, but aided or made more severe by cyber means. And third, misinformation and disinformation attacks can target industries or brands and negatively impact their business prospects. Beyond the cyber domain, threats to industry with national security implications include forced joint ventures and physical threats to travelers or foreign staff.

Available Resources

Different segments of the private sector, as well as individual entities, have different needs, constraints, and capacities to defend against and respond to cyber events or incidents. Public, private, and collaborative organizations with cybersecurity-related mandates have proliferated in recent years, but victims sometimes struggle to know who to contact for what types of issues or concerns. Confusion can be heightened during a crisis. Primary collaborative forums and resources include:

Department of Justice (DoJ)/Federal Bureau of Investigation (FBI). The FBI, as well as the National Cyber Investigative Joint Task Force (NCI-JTF), has important investigatory authorities and a mandate to lead in "threat response," according to roles outlined in Presidential Policy Directive (PPD)-41. This includes "identifying threat pursuit and disruption opportunities."[5]

Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA). DHS is charged with coordinating the "overall Federal effort to promote the security and resilience of the Nation's critical infrastructure."[6] DHS is also the lead organization for "asset response," which includes a variety of functions such as "assessing potential risks to the

[5] *See Presidential Policy Directive – United States Cyber Incident Coordination*, White House (July 26, 2016),https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.

[6] *See Presidential Policy Directive – Critical Infrastructure Security and Resilience*, White House (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[targeted] sector or region, including potential cascading effects," and related activities as described in PPD-41.[7] Increasingly, CISA looks to proactively coordinate with key industry players through the Joint Cyber Defense Collaborative (JCDC), of which CrowdStrike serves as one of the 9 founding "plankholder" members.

Sector Risk Management Agencies (SRMAs). These agencies serve as the regular federal interface for the collaboration and coordination with sector specific critical infrastructure entities, and at times advance new regulatory requirements and share information about threats to respective sectors, including cyber threats.

Sector Coordinating Councils (SCCs), and Information Sharing and Analysis Centers (ISACs)/Information Sharing and Analysis Organizations (ISAOs). These organizations exist to facilitate industry collaboration at the sector-level or for particular functions or events. Some companies participate in multiple such structures, and each operate somewhat differently according to stakeholder needs and expectations.

Intelligence structures. In recent years, intelligence organizations have sought to communicate risks and threats more publicly to alert wider audiences. With respect to cybersecurity, NCSC and its antecedents have highlighted foreign intelligence services as a key threat. The National Security Agency's (NSA) Cybersecurity Collaboration Center (CCC) seeks to coordinate with industry "to prevent and eradicate foreign cyber threats to National Security Systems (NSS), the Department of Defense, and the Defense Industrial Base (DIB)."[8]

Private sector. Sometimes lost in this array of partnership opportunities and mechanisms is a fundamental reality of the cybersecurity landscape. When a private company is the victim of a breach or cyberattack, and it cannot remediate the issue independently, it must turn to a private sector incident response (IR) provider. There is no U.S. government agency that has the authorities and capabilities to hunt for adversaries across a victim IT environment, eject them, identify and resolve the attack vector, and help maintain or restore the victim's operations.

Cybersecurity and Counterintelligence

Numerous government entities have realigned and reformed in recent years to support cyber missions. The Committee's report describes the establishment of the National Counterintelligence and Security Center (NCSC) in 2014[9] and covers existing cybersecurity mandates. More recently, the Central Intelligence Agency (CIA) created the Directorate for Digital Innovation (DDI) in 2015;[10] CISA was formally established in 2018;[11] NSA launched the

---

[7] These roles are also enumerated within PPD-41 and the National Incident Response Plan.
[8] *See generally NSA Cybersecurity Collaboration Center*, https://www.nsa.gov/About/Cybersecurity-Collaboration-Center/.
[9] *See generally History of the National Counterintelligence and Security Center (NCSC)*, https://www.dni.gov/index.php/ncsc-who-we-are/ncsc-history.
[10] *See* Sean Lyngaas, *Inside the CIA's New Digital Directorate*, FCW (Oct. 1, 2015), https://fcw.com/security/2015/10/inside-the-cias-new-digital-directorate/207156/.
[11] *See generally, About CISA*, https://www.cisa.gov/about-cisa.

Cybersecurity Collaboration Center (CCC) in 2020;[12] and Office of the National Cyber Director (ONCD) was created in 2021[13]–all in an attempt to better address cyber threats.

As you consider options to clarify or strengthen NCSC roles and missions, consider a few key functions. First is raising awareness at a leadership level about threats. Because threats evolve and new executives are minted every day, this mission area must be a continuous function to maintain rather than a task to be completed.

Second, NCSC may be able to process and disclose industry-relevant insights from Intelligence Community (IC) information or assessments. The most actionable information would relate to new taskings for foreign intelligence services or developments in targeting practices. (Industry and academia do develop their own points of view on these issues, and in certain instances may develop higher-quality or more timely information than that possessed by the government.) But NCSC can contribute to stakeholders' understanding by adding additional insights where possible.

Perhaps some useful intelligence along these lines is classified. And perhaps some portions ought to remain classified in order to protect sensitive sources and methods. But disclosing some types of information does not inevitably compromise collection details. Notably, government disclosures this year regarding Russian plans and intentions for Ukraine, including warnings about specific disinformation themes and advisories about specific cyber threats, were well-received by industry. Based on this intelligence, many organizations did take proactive measures to harden defenses. Others would be better suited to characterize effects on IC activities from such disclosures, but these examples illustrate how to communicate sensitive threats clearly and openly.

Third, NCSC should endeavor to operate at scale. The private sector is enormous, and engagement efforts that are not either targeted extremely precisely or available to thousands of recipients will probably fail to make systemic impacts. This is another argument in favor of optimizing for making information–even sensitive information–widely available. Too often, conversations about cyber collaboration devolve into tactical plans for clearing more people or providing classified infrastructure to industry recipients. Aside from the costs and operational burdens associated with such proposals, they will not scale to protect most potential victims.

Seeking scale also means NCSC should feel comfortable–and probably prefer–leveraging intermediaries to broaden its impact. This might include existing government structures like JCDC. Or it might mean use of commercial service providers to distribute warnings to, or implement defenses for, their customers or stakeholder communities.[14] Where IC organizations

---

[12] *See NSA's Cybersecurity Collaboration Center Celebrates its First Year*, NSA (Dec. 22, 2021), https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/2881886/nsas-cybersecurity-collaboration-center-celebrates-its-first-year/.

[13] *See generally Office of the National Cyber Director*, White House https://www.whitehouse.gov/oncd/.

[14] *See George Kurtz*, *Questions for the Record - Hearing on the Hack of U.S. Networks by a Foreign Adversary*, Senate Select Committee on Intelligence (Feb. 23, 2021 at 1-3)(How the private sector has

consume private sector threat intelligence, doing so in a shared services model with broad distribution entitlements can expand reach and assist the greatest number of stakeholders.

Elevating Defenses

The cybersecurity community, spanning public and private actors, is consistently engaged in efforts to strengthen cybersecurity and resilience. Informed observers agree that we must make further improvements. Several lines of effort are worth noting here:

Private sector developments. The cybersecurity industry moves quickly to address emerging threats, and sophisticated private sector entities quickly integrate new solutions. The most impactful security concepts and controls of recent years, like those mandated for federal use by E.O. 14028 (i.e, Endpoint Detection and Response (EDR) and adoption of Zero Trust Architectures, as well as comprehensive approaches to logging security-relevant information) were forged by the private sector in private sector settings.[15] Adoption is still uneven across industry, but is trending in the right direction.

During my time at CrowdStrike, some of the most impactful changes I've seen have involved the advent of groundbreaking managed threat hunting services and broader managed security services, including managed identity services. Increasingly, this has become an industry-wide trend that responds to customer preferences to engage professionals to provide a reliable, consistently-high degree of protection on a 24 hours per day, 7 days per week, 365 days per year basis. Some organizations use these capabilities to overlay or augment existing security teams, others free up capacity for existing staff to focus on security program maturity or conducting proactive risk mitigation activities. As with other efficiencies, organizations recognize that effective risk mitigation does not require doing everything 'in-house.'

Streamlining and enhancing government services. Large and sophisticated private sector entities are aware of and participate in multiple collaboration structures. Participation can be time-consuming, and discussions can cover a wide variety of topics, some of which are more appropriate for certain corporate roles than others (discussions may span topics relevant to Executive, Security Subject Matter Expert, Legal, Compliance, and other personas). At a certain point, the creation of new structures can create 'noise' and dilute participation potential, so government entities should be extremely clear about the value proposition of any new entities. Efforts to reduce or abstract away existing complexity would be helpful for small and medium sized enterprises in particular.

Subject to these constraints, it is worth considering additional government programs or efforts that make available concrete cybersecurity services, beyond consultation and collaboration, to

---

promoted practical information sharing), https://www.intelligence.senate.gov/sites/default/files/documents/qfr-gkurtz-022321.pdf.

[15] *See George Kurtz*, *Testimony on Cybersecurity and Supply Chain Threats*, Senate Select Committee on Intelligence (Feb. 23, 2021 at 3-5)(Extended discussion on emerging cybersecurity controls and practices), https://www.intelligence.senate.gov/sites/default/files/documents/os-gkurtz-022321.pdf.

certain entities. As a community, we should undertake a more serious conversation about expanding national Incident Response (IR) capacity. IR demand is incredibly elastic, and IR supply is relatively fixed. Broad-based, concurrent cyberespionage campaigns in 2021 with thousands of victims did strain national capacity. The best practice for private entities is to have an IR retainer in place, so a skilled provider can offer assistance within a stipulated time frame, and under other terms outlined in a Service Level Agreement (SLA). A program that retained skilled providers in advance for use during significant cyber incidents could expand the cybersecurity workforce and strengthen national resilience. Eligibility for benefits under such a program would likely be based on need or vulnerability (e.g., for small businesses), and/or on criticality (e.g, entities with a national security nexus or critical infrastructure entities with systemic importance).

Incentives. Over the years, policymakers and industry groups have cited tax incentives, such as tax deductions or credits, as a possible driver for increased cybersecurity investment. To date, these proposals at the federal level have stalled out. But such mechanisms have proven effective in shaping behavior in other domains and are worth consideration here.

Government procurement can be a vehicle for innovation in the security space. The Federal government is a large consumer of cybersecurity services and does leverage acquisition requirements to drive cybersecurity outcomes. This, in turn, shapes the broader ecosystem. This is appropriate, but contracting officials must be careful not to create insurmountable barriers to the adoption of new and more innovative providers, nor continue to reward providers delivering consistent vulnerabilities into government networks. From the perspective of a new company offering a new type of product or service, overwrought or overly-prescriptive procurement guidelines can operate as a barrier. This can also reduce security in some cases.

Regulatory approaches. Over the past 20 years, policymakers and industry groups have struggled to come to terms with the optimal role for regulation to drive better cybersecurity outcomes. At this point, the key questions are familiar. *Given that some adversaries have the resources of a state behind them, can any regulation successfully prevent a breach? Given that government entities suffer breaches from time to time, can they credibly advance regulatory guidance? Past a certain point, do additional regulations become compliance exercises with deleterious effects on security? Will specific regulations stifle innovation surrounding better approaches to security?*

Perhaps we will not today resolve these questions to the satisfaction of the entire cybersecurity community. But a few points are clear. First, cybersecurity is a shared responsibility, and private entities should take reasonable steps to secure themselves and their data. Defining ‘reasonable’ can be a challenge, but regulations that adopt a principles-based approach are better designed to evolve more quickly than those that mandate specific controls, which can become obsolete in light of new threats. Second, clear and consistent incident response requirements can improve cyber incident response practices in private sector organizations. At present, the scope and particulars of new requirements to report certain incidents to CISA are not quite resolved, and the SEC is currently evaluating new requirements for listed companies, which could create an

entirely different reporting threshold framework. Although well-intended, too many simultaneous efforts could create gaps, overlaps, or confusion. At a minimum, we must pay special attention, and make adjustments if needed, to avoid these outcomes. It is both unreasonable and impractical to expect the government to solve every cybersecurity problem, but the government can play a unique role in incentivizing the adoption of best practices and technologies.

Conclusions

Thank you again for the opportunity to testify today. The cybersecurity industry and stakeholder community have made significant strides in recent years to defend against all manner of cyber threats, including those from nation-state actors. But we have more work to do, and we must work together to ensure we're surfacing practical solutions. These solutions must reach scale in order to meet the magnitude of the threat. And we must make special efforts to ensure that help reaches the small and medium sized enterprises that need it most.

I would like to conclude with a reminder that the problems I've described here affect not just the United States, but developed and developing nations around the world. At this point, it is already clear that success or failure in meeting these challenges will tell some part of the story of how nations will rise and fall in the 21st century. Thank you, and I look forward to your questions.

###