SHIELD
by SOURCEREE

What's Inside

National Security Newsletter

May 2021

SOURCEREE

For May's SHIELD Newsletter, the Sourceree team took a deep dive into the information and communications technology (ICT) supply chain. In beginning of 2021, the US Government has focused initiatives and introduced legislation to secure the ICT supply chain to secure semiconductors, printed circuit boards (PCBs), and cybersecurity in the energy sector. We open with some recommendations on how to govern and guide the ICT supply chain from the Information Technology Industry Council, then we examine some real-world examples of why their recommended comprehensive approach with public-private collaboration is necessary. The global semiconductor shortage has been looming for the better part of a year, and we provide a series of articles outlining the US government's next steps supported by industry leaders, as well as some farther-reaching national security fears held by US and Taiwanese chip manufacturers. Next, US Congress has taken steps to propose securing the use and acquisition of offshore-produced PCBs, and we outline the market share and some potential vulnerabilities identified by an industry spokesperson. And finally, beyond the goods themselves is the capability to secure our cyber infrastructure against attack. The Colonial Pipeline ransomware attack caught the country off guard, but with a likelihood of swift, high payouts for ransomware attacks, should it have? Leveraging public-private collaboration to take a comprehensive look at the variety of threats posed to our ICT apparatus is the only way to secure our national security and industry.

--Adam Murphy, Sourceree President

Supply Chain Security: Principles for Strategic Review

The Information Technology Industry Council (ITI)
18 March 2021

Select excerpts from the piece:

Over the past several years, uncoordinated approaches by the U.S. federal government to information and communications technology (ICT) supply chain risk management have resulted in a patchwork of overlapping, inconsistent and, in some cases, conflicting measures, including Executive Orders, agency actions, regulations and legislation. Currently, there are upwards of 30 supply chain security measures being contemplated and/or in force, resulting in a confusing supply chain security policy terrain that is increasingly difficult for companies to navigate, and which in many respects has not achieved the intended goal of improved supply chain security and resilience across the U.S. federal enterprise, critical infrastructure, and global private sector ICT supply chains.

To streamline and improve these varied efforts, ITI recommends the U.S. government takes into account the following principles:

- Designate a lead supply chain security risk management agency and empower the National Cyber Director to coordinate these efforts.
- Take a risk-based and evidence-driven approach and facilitate transparency and predictability for private actors to the greatest extent possible.
- Leverage the existing ICT Supply Chain Risk Management Task Force as a focal point for public-private collaboration on supply chain security.
- View supply chain risk management through the lens of trustworthiness, which has many dimensions.
- Ensure bi-directional information-sharing is a key tenet in any supply chain security approach.
- Use measures to advance and protect U.S. national security objectives without putting American competitiveness at risk.

The Semiconductor Shortage & Global Security

In May 2021, the Semiconductors in America Coalition (SIAC), a coalition of semiconductor companies and downstream users of semiconductors, was founded with a mission to bolster America's economy, critical infrastructure, and national security by advancing semiconductor manufacturing and research in the US. In SIAC's letter to Congress, urging support of the CHIPS for America Act, they write: "Semiconductors are crucial to the technologies of today and tomorrow, including aerospace, automotive, cloud computing, medical devices, telecommunications, and more. Semiconductors also underpin many of the technologies and systems vital to our national security and critical infrastructure."[1] The surging demand in 2021 for items that use chip technology has placed the global shortage into sharp focus.

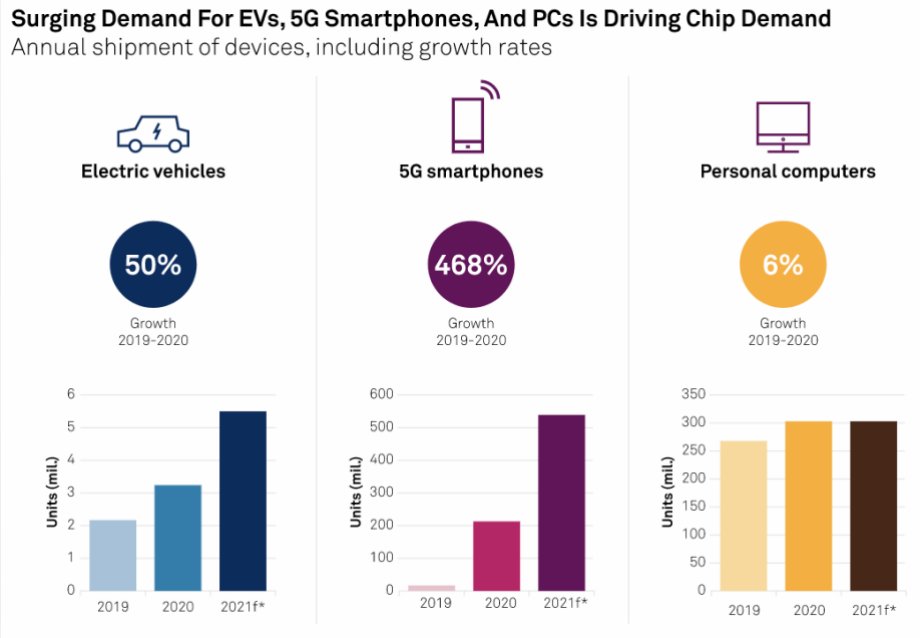

Image Source, S&P Global: Global Chip Shortage Engulfs A Growing List Of Tech Players

Among SIAC's talking points in support of the CHIPS for America Act include the increasing cost of operating a semiconductor fab in the United States – 20-40% more expensive than overseas – due to other governments offering industry subsidies. As a result, US semiconductor manufacturing has dropped from 37% of the global share in 1990 to only 12% today.[2]

Taiwan and the Silicon Shield

Taiwan Semiconductor Manufacturing Company (TSMC), one of the world leaders in manufacturing chips, approved $100 Billion for capacity expansion over the next three years in response to the shortage and overall growing demand. TSMC's CEO stated that its fabs had been operating at over 100% for the 12 months and still not meeting demand.[3]

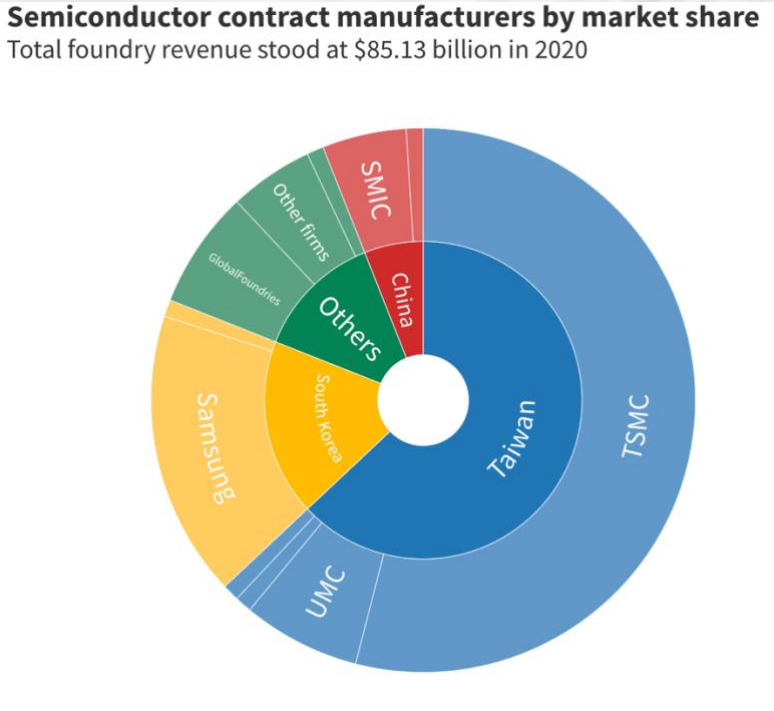

Image Source, CNBC Citing TrendForce: Dependence on Taiwan for Semiconductors

In a *60 Minutes* interview examining the chip shortage and the future of the semiconductor industry, Intel CEO Pat Gelsinger compared the United States' interest in Taiwan's ability to maintain sovereignty from the People's Republic of China (PRC) as similar to US involvement in Iraq, defending Kuwait. Gelsinger stated that today's oil is chips. TSMC Chairman Mark Liu defined the "Silicon Shield" as the world's reliance on Taiwan for semiconductor manufacturing as a strong enough incentive to protect Taiwan from PRC aggression.[4]

The US Response

In April 2021, US President Joseph Biden participated in a virtual meeting on the ongoing chip shortage that featured executives from 19 companies.[5] As part of his multi-trillion-dollar infrastructure plan, President Biden has allocated $50 billion to the semiconductor industry. The plan aims to repatriate semiconductor production from countries such as Japan, South Korea, Taiwan, and China.[6]

Offshore Manufacture of Printed Circuit Boards

The global shortage and offshore control of the fabrication and assembly of technologies like semiconductors has prompted a US Senator to propose restrictions against the Department of Defense using of printed circuit boards (PCBs) manufactured by adversary nations. The amendment to the National Defense Authorization Act (NDAA) identifies "adversary nations" as China, Russia, Iran, and North Korea.[7] One company estimates the global market for PCBs will increase from $57.7 billion in 2020 to $69.5 billion by 2024.[8] The long-term effects of a global shortage during the COVID-19 pandemic, particularly during the shutdown and restrictions on assembly workforces, combined with a renewed interest in a US-based supply chain for advanced technologies makes this an issue worth monitoring for the next several years.

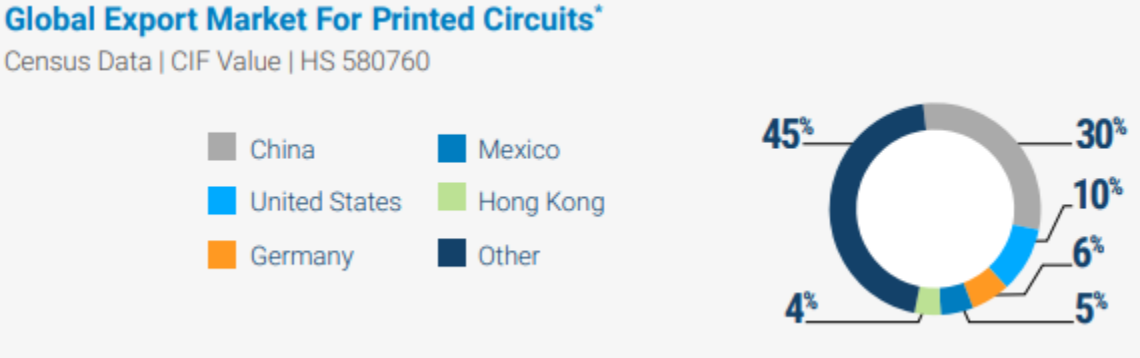

Image Source, Descartes: U.S. Supply Chain Vulnerability Analysis

Chris Mitchell of the Institute for Printed Circuits (IPC), outlines PCBs' four primary security vulnerabilities[9]:

- Malicious insertion of components into PCBs;
- Quality control issues, mitigated by a trusted supply chain;
- Intellectual property theft caused by a manufacturer's need to know about the operating system for a PCB's intended use; and
- Overall resiliency of the US electronics manufacturing ecosystem.

Ransomware's Effect on Supply Chain and Critical Infrastructure

The Department of Treasury published a report in October of 2020 citing the FBI research indicating there was a 37 percent annual increase in reported ransomware cases and a 147 percent annual increase in associated losses from 2018 to 2019.[10] Ransomware is a type of malware that holds information or systems hostage via encryption until the victim pays the attackers for its release. Vulnerable to ransomware attacks, along with essentially every other sector in the United States, is the US supply chain for critical materials and infrastructure. In the May 2021 ransomware attack on Colonial Pipeline Co. placed 45% of the US East Coast fuel supply at risk, forcing Colonial's CEO to make the decision to pay the $4.4 million ransom.[11]

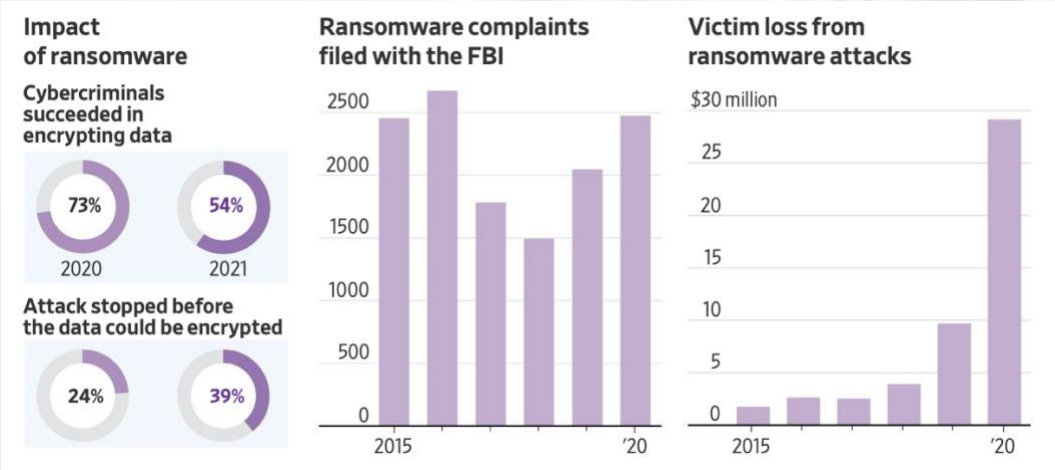

Image Source, WSJ: U.S Pipeline Shutdown Exposes Cybersecurity Threat to Energy Sector

In 2020 and early 2021, ransomware attacks have targeted and received payments from the travel, finance, automobile, education, and technology companies, including:

- Kia Motors America 2021 – $20 million raised to $30 Million;[12]
- Travelex 2020 – $2.3 Million;[13]
- University of California, San Francisco 2020 – $1.14 Million;[14]
- CWT Global 2020 – $4.5 Million;[15]
- Garmin 2020 – $10 Million.[16]

The US Response

In the wake of Colonial Pipeline incident, the US House Committee on Energy and Commerce reintroduced bipartisan legislation aimed at bolstering the Department of Energy's (DOE) ability to respond to cybersecurity threats to the US energy infrastructure.

> "1. The Pipeline and LNG Facility Cybersecurity Preparedness Act, which would require DOE to implement a program to coordinate federal agencies, states, and the energy sector to ensure the security, resiliency and survivability of natural gas pipeline, hazardous liquid pipelines and liquefied natural gas ("LNG") facilities;

2. The Energy Emergency Leadership Act, which would require the Secretary of Energy to assign energy emergency and energy security functions to an Assistant Secretary, including responsibilities regarding infrastructure and cybersecurity;

3. The Cyber Sense Act and the Enhancing Grid Security through Public-Private Partnerships Act, which directs the Secretary of Energy to establish a voluntary Cyber Sense program to test the cybersecurity of products and technologies intended for use in the bulk-power system; and

4. The Enhancing Grid Security through Public Private Partnerships Act, which directs the DOE to implement programs to address cybersecurity-related vulnerabilities of, and physical threats to, the electric grid."[17]

Sources

[1] SIAC Letter to Congressional Leaders in Support of the CHIPS Act
[2] SIAC Letter to Congressional Leaders in Support of the CHIPS Act
[3] TSMC to Spend $100 Billion Over Three Years to Grow Capacity
[4] Chip shortage highlights U.S. dependence on fragile supply chain
[5] 'This is infrastructure': Biden talks up money for semiconductor industry while meeting with 19 companies on chip shortage
[6] U.S. needs to invest in semiconductor 'infrastructure,' Biden tells business leaders facing crippling shortages
[7] Hawley bill would spotlight Chinese electronics in defense systems
[8] Global Printed Circuit Boards Market to Be Worth $69.5 Billion by 2024, Says Beroe Inc
[9] NDAA requires Pentagon to secure circuit board supply chain
[10] Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments
[11] Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom
[12] Kia Motors America Suffers a $20 Million Suspected DoppelPaymer Ransomware Attack
[13] Travelex Paid $2.3 Million to Ransomware Gang: Report
[14] The University Of California Pays $1 Million Ransom Following Cyber Attack
[15] 'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals
[16] Incident Of The Week: Garmin Pays $10 Million To Ransomware Hackers Who Rendered Systems Useless
[17] Government Races to Secure Critical Infrastructure in Wake of Colonial Pipeline Ransomware Attack

Protected by

SHIELD
by SOURCEREE

Sourceree's SHIELD program is a comprehensive supply chain risk management (SCRM) solution designed to help answer questions about supply chain disruptions and risks, particularly foreign investment.

SHIELD VISION

Software platform for on-demand supply chain risk assessments and financial intelligence

SHIELD SQUAD

Analytical Support

SHIELD INTEL

Business intelligence reports on critical suppliers