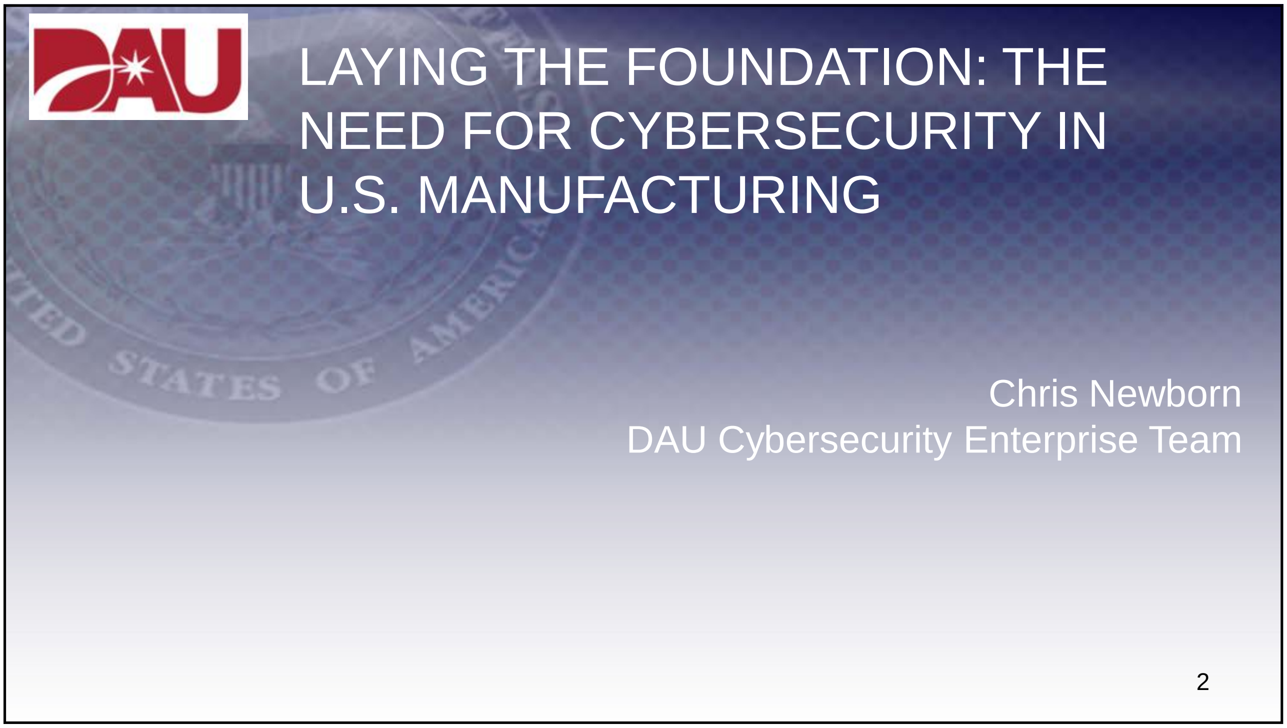


LAYING THE FOUNDATION: THE NEED FOR CYBERSECURITY IN U.S. MANUFACTURING

Chris Newborn
DAU Cybersecurity Enterprise Team

2

2

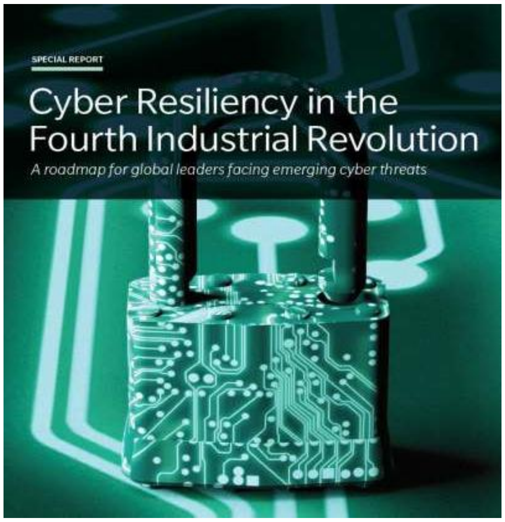
Outline

- **Why the Need for Cybersecurity**
  - Cyber Crime Damages
  - Verizon Data Breach Investigation Report (VBIR)
  - Geographical Heat Maps
  - Legislation
- **How and Why Threats are Impacting US Manufacturing**
  - Threats to Manufacturers
  - Supply Chain Example
  - Attacker's & Defender's Dilemma
  - Cybersecurity Challenge
  - Cyber Espionage
  - Observations and Assumptions
- **What is New in Cybersecurity**
  - 2020 Cyberthreat Report
  - Road Ahead: Cybersecurity in 2020 & Beyond
  - Government Future Assessments
  - Best Practices
  - Delivered Uncompromised – MITRE Report
- **Summary**

3

3

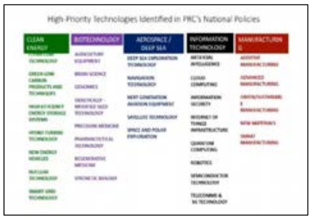
Why the Need for Cybersecurity?


SPECIAL REPORT
Cyber Resiliency in the Fourth Industrial Revolution
A roadmap for global leaders facing emerging cyber threats

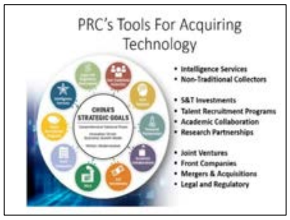
Why Cybersecurity

FBI is investigating more than 1,000 cases of Chinese theft of US technology

"They've pioneered an expansive approach to stealing innovation through a wide range of actors, including not just Chinese intelligence services but state-owned enterprises, ostensibly private companies, certain kinds of graduate students and researchers, and a whole variety of other actors all working on their behalf."


High-Priority Technologies Identified in PRC's National Policies

CLEAN ENERGY	BIOTECHNOLOGY	AEROSPACE / DEEP SEA	INFORMATION TECHNOLOGY	MANUFACTURING
TECHNOLOGY	AGRICULTURE EQUIPMENT	DEEP SEA EXPLORATION TECHNOLOGY	ARTIFICIAL INTELLIGENCE	ADDITIVE MANUFACTURING
GREEN LOW CARBON PRODUCTS AND TECHNIQUES	BRAIN SCIENCE	NAVIGATION TECHNOLOGY	CLOUD COMPUTING	ADVANCED MANUFACTURING
HIGH EFFICIENCY ENERGY STORAGE SYSTEMS	GENOMICS	NEXT GENERATION AVIATION EQUIPMENT	INFORMATION SECURITY	GREEN/SUSTAINABLE MANUFACTURING
HYDRO TURBINE TECHNOLOGY	GENETICALLY-MODIFIED SEED TECHNOLOGY	SATELLITE TECHNOLOGY	INTERNET OF THINGS INFRASTRUCTURE	NEW MATERIALS
NEW ENERGY VEHICLES	PRECISION MEDICINE	SPACE AND POLAR EXPLORATION	QUANTUM COMPUTING	SMART MANUFACTURING
NUCLEAR TECHNOLOGY	PHARMACEUTICAL TECHNOLOGY		ROBOTICS	
SMART GRID TECHNOLOGY	REGENERATIVE MEDICINE		SEMICONDUCTOR TECHNOLOGY	
	SYNTHETIC BIOLOGY		TELECOMMS & 5G TECHNOLOGY	

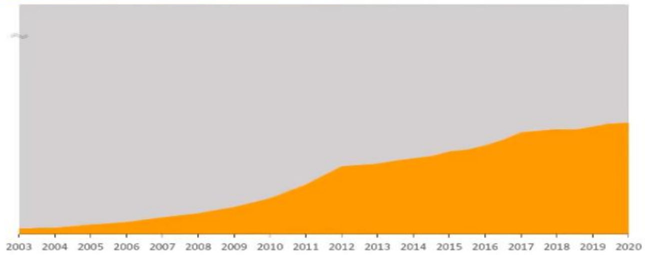

PRC's Tools For Acquiring Technology

- Intelligence Services
- Non-Traditional Collectors

- S&T Investments
- Talent Recruitment Programs
- Academic Collaboration
- Research Partnerships

- Joint Ventures
- Front Companies
- Mergers & Acquisitions
- Legal and Regulatory

FBI Technology Theft Cases Involving China



Cybercrime Damages $6 Trillion By 2021

Cybercrime is the greatest threat to every company in the world, and one of the biggest problems with mankind. The impact on society is reflected in the numbers. Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined. The damage cost projections are based on historical cybercrime figures including recent year-over-year growth, a dramatic increase in hostile nation state sponsored and organized crime gang hacking activities, and a cyber attack surface which will be an order of magnitude greater in 2021 than it is today. Cybercrime costs include damage and destruction of data, stolen money, lost productivity, theft of intellectual property, theft of personal and financial data, embezzlement, fraud, post-attack disruption to the normal course of business, forensic investigation, restoration and deletion of hacked data and systems, and reputational harm.

2019 Verizon Data Breach Investigations Report (DBIR)

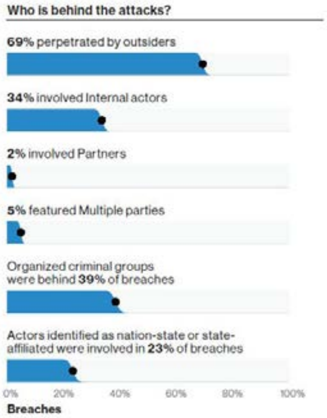


Figure 1.

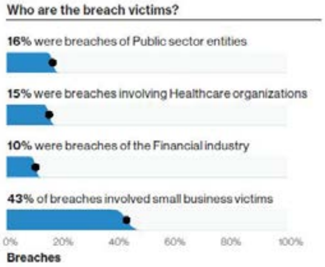


Figure 2.

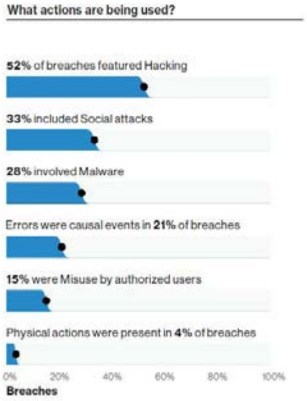
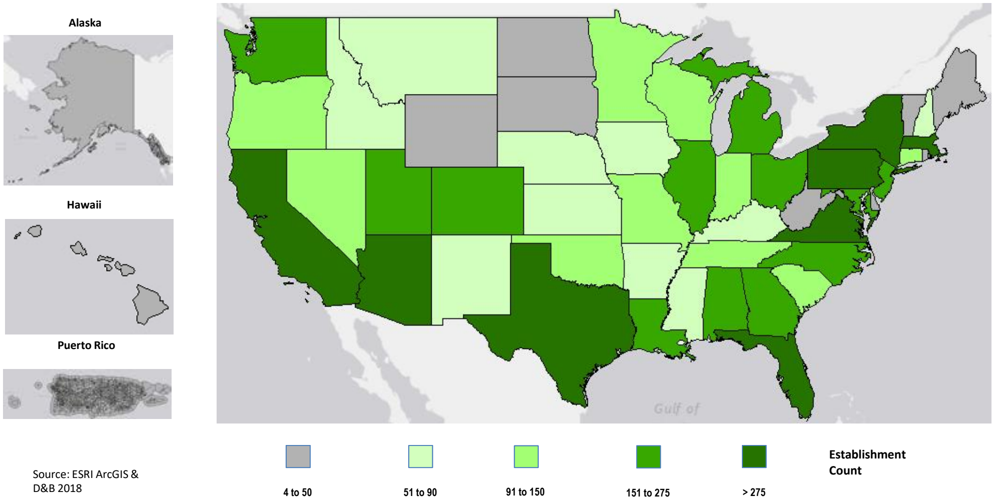


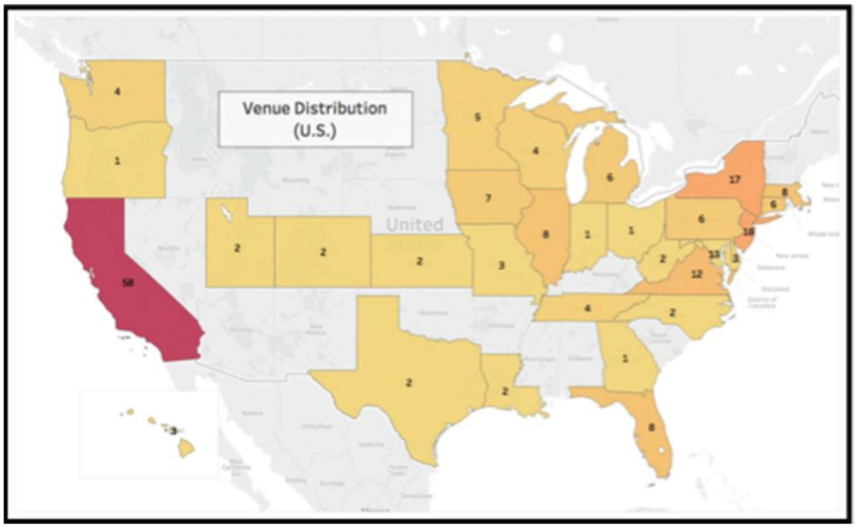
Figure 3.

DOD Related Manufacturing Companies



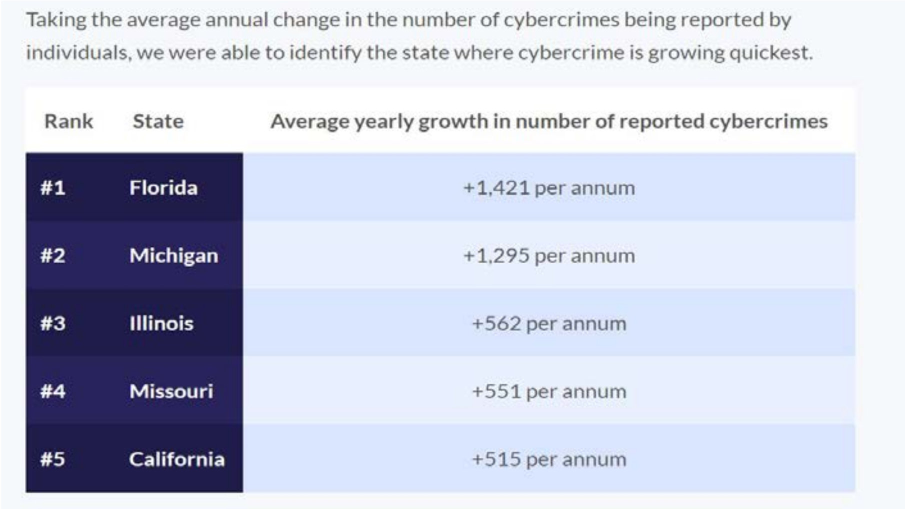
Source: ESRI ArcGIS & D&B 2018

Distribution of Chinese Espionage Cases in the United States



https://breakingdefense.com/2018/12/how-to-combat-chinese-espionage-ip-theft-nick-eftimiades-top-intel-expert/

Which state’s cybercrime is growing the fastest?



Taking the average annual change in the number of cybercrimes being reported by individuals, we were able to identify the state where cybercrime is growing quickest.

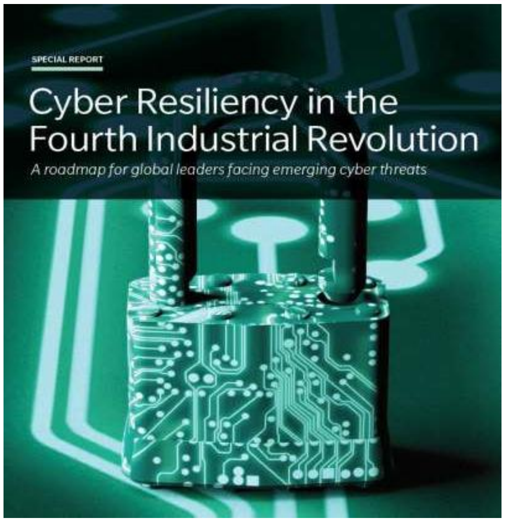
Rank	State	Average yearly growth in number of reported cybercrimes
#1	Florida	+1,421 per annum
#2	Michigan	+1,295 per annum
#3	Illinois	+562 per annum
#4	Missouri	+551 per annum
#5	California	+515 per annum

Cybersecurity Legislation 2019

2019 Introductions: At least 43 states and Puerto Rico introduced or considered close to 300 bills or resolutions that deal significantly with cybersecurity. Thirty-one states enacted cybersecurity-related legislation in 2019 (the status of enacted bills are highlighted in bold). Some of the key areas of legislative activity include:

- Requiring government agencies or businesses to implement training or specific types of security policies and practices
- Creating task forces or commissions
- restructuring government for improved security
- studying the use of blockchain for cybersecurity
- providing for the security of utilities and critical infrastructure
- exempting cybersecurity operations information from public records laws
- addressing the security of connected devices
- regulating cybersecurity within the insurance industry
- Providing funding for improved security measures (note: this page does not list all cybersecurity appropriations bills; rather, it focuses on those that include specific mandates or projects to be funded)
- addressing cybersecurity threats to elections (see NCSL's Elections data base for other types of elections security-related legislation).

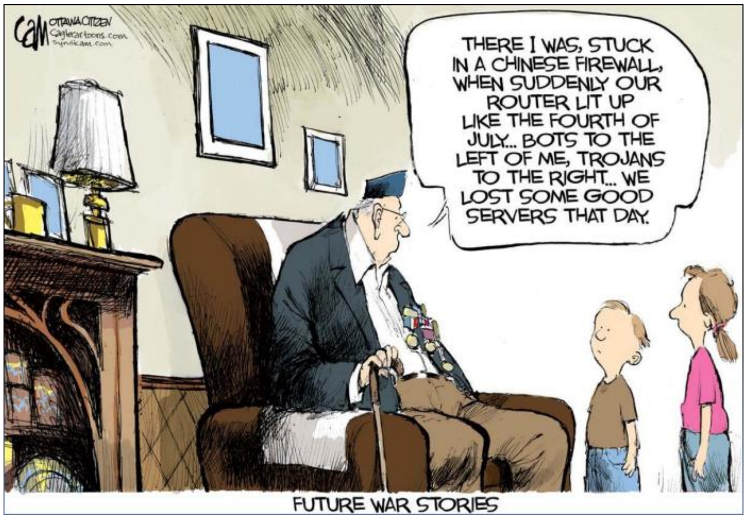
How and Why Threats are Impacting US Manufacturing



SPECIAL REPORT

Cyber Resiliency in the Fourth Industrial Revolution

A roadmap for global leaders facing emerging cyber threats


CAM OTTAWA CITIZEN
caglecartoons.com
syndicam.com
THERE I WAS, STUCK IN A CHINESE FIREWALL, WHEN SUDDENLY OUR ROUTER LIT UP LIKE THE FOURTH OF JULY... BOTS TO THE LEFT OF ME, TROJANS TO THE RIGHT... WE LOST SOME GOOD SERVERS THAT DAY.
FUTURE WAR STORIES

The 5 Most Common Cybersecurity Threats to Manufacturers

1. Identity Theft

People are most familiar with the identity theft that happens when hackers get their Social Security Numbers and use them to apply for loans or lines of credit. When it comes to the manufacturing sector, problems arise if hackers break into a customer database with help from malware and access customer data, which can potentially be used to practice identity theft.

2. Phishing

Phishing occurs when cybercriminals craft convincing emails and use them to trick recipients into revealing sensitive information such as passwords. These messages often have branded letterheads or similar elements to help persuade people of their legitimacy. Phishing emails generally target a wide audience and are fairly easy to spot with generic greetings such as "Dear valued customer."

3. Spear Phishing

Spear phishing is a highly targeted kind of phishing that may only address one person at a manufacturing company or people within a particular department. In contrast to the phishing attempts previously mentioned, these targeted messages are more specialized and relevant to the recipient.

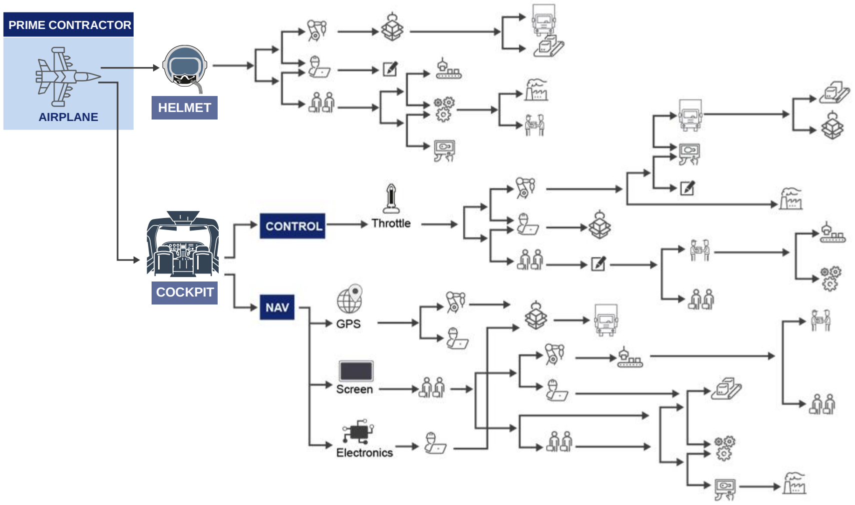
4. Spam

Spam messages are annoying for everyday people, but they can substantially reduce productivity at manufacturing plants. At one Dunlop Industrial plant in South Africa, members of the IT team had to manually sort through approximately 12,000 spam messages a day — a task that required up to 90 minutes and kept them from more effective uses of their time.

5. Compromised Webpages

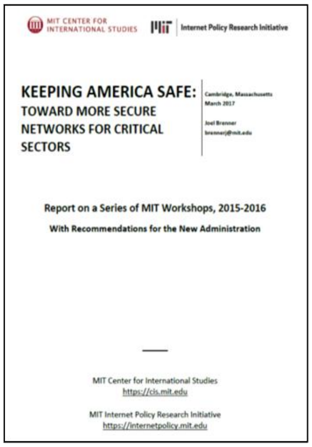
Webpage compromises happen when hackers take control of websites and either make them inoperable or fill them with misleading content to fool customers. Sometimes, hackers embed programs that automatically install dangerous files on site visitors' computers without their knowledge. These situations can severely damage the reputations of the impacted manufacturing companies.

Risk: DoD Has a Highly Complex Multi-tier Supply Chain (example only)



All Contractors Need to Do Their Part to Protect Information

Cyber Paradox: Tech vs People



MIT CENTER FOR INTERNATIONAL STUDIES | MIT | Internet Policy Research Initiative

KEEPING AMERICA SAFE:
TOWARD MORE SECURE
NETWORKS FOR CRITICAL
SECTORS

Cambridge, Massachusetts
March 2017

Joel Brenner
brennerj@mit.edu

Report on a Series of MIT Workshops, 2015-2016

With Recommendations for the New Administration

MIT Center for International Studies
https://cis.mit.edu

MIT Internet Policy Research Initiative
https://internetpolicy.mit.edu

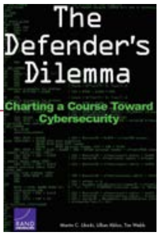
1. "It is a serious error to assume that cybersecurity is entirely a matter of **technical specifications and system design**.
2. **Poor business management, lack of clear responsibility** within organizations, and **bad user behavior** would continue to create significant vulnerabilities even if the technical issues could suddenly be fixed.
3. Last year, when for the first time the Bank of England included **cybersecurity as a major risk factor** for the financial stability of the United Kingdom, its number one finding was, "**Overemphasis on technological** (as opposed to management, behavioral and cultural) aspects weakens cyber defensive capabilities." (p. 23)

Which has greater Impact on cybersecurity?

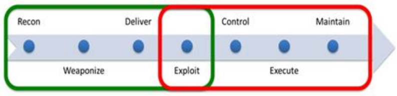
1. Technology

2. People

Attacker's /Defender's Dilemma



- **Defender has some advantages:**



1. Kill Chain disrupted at any link

2. Rapidly acquire & insert new technology

3. Emerging & innovative technologies

4. Crowdsourcing, vulnerability discovery & pen-testing

- **Attacker has some advantages too:**

1. Many Access Paths

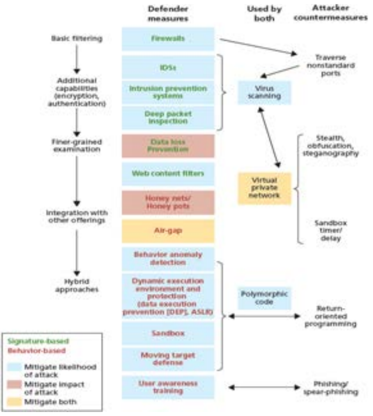
2. Human Behavior

3. Supply Chain

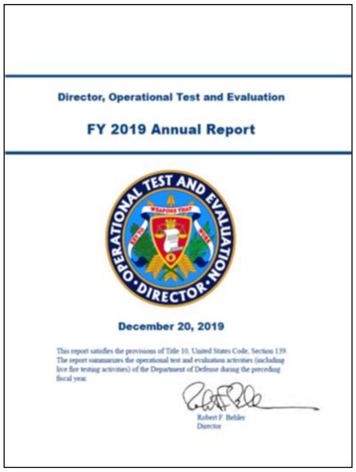
4. Cost

5. Zero Day

6. Bugs


Defender measures
Used by both
Attacker countermeasures
Basic filtering
Additional capabilities (encryption, authentication)
Finer-grained examination
Integration with other offerings
Hybrid approaches
Firewalls
IDSs
Intrusion prevention systems
Deep packet inspection
Data loss Prevention
Web content filters
Honey nets/ Honey pots
Air-gap
Behavior anomaly detection
Dynamic execution environment and protection (data execution prevention [DEP], ASLR)
Sandbox
Moving target defense
User awareness training
Virus scanning
Virtual private network
Polymorphic code
Traverse nonstandard ports
Stealth, obfuscation, steganography
Sandbox timer/ delay
Return-oriented programming
Phishing/ spear-phishing
Signature-based
Behavior-based
Mitigate likelihood of attack
Mitigate impact of attack
Mitigate both

Cybersecurity Challenge



Director, Operational Test and Evaluation

FY 2019 Annual Report

December 20, 2019

This report satisfies the provisions of Title 10, United States Code, Section 139. The report summarizes the operational test and evaluation activities (including live fire testing activities) of the Department of Defense during the preceding fiscal year.

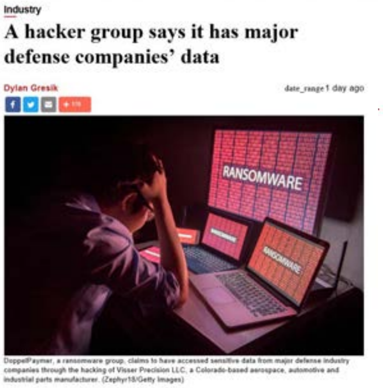
Robert F. Behler
Director

“Breaches of Contractors Give Advantage to Adversary”

- Breaches of cleared defense contractors provide adversaries with information that enables the development of cutting-edge weapons to be used against us, paves the way for cyber-attacks that could compromise critical DOD missions, and degrades our technical and commercial advantages.
- DOT&E analyzed past breaches of defense contractors for several major programs and found that these breaches exposed extensive information that empowers our adversaries to degrade key DOD systems and missions. DOT&E also observed several supply-chain table top exercises where significant efforts were being implemented to help shield critical design information and software from adversaries. Efforts such as these should be implemented for all critical programs, and operational assessments and monitoring of contractor networks, tools, facilities, and software factories should become routine for critical programs.” (p. 230)

Cyber Espionage

- “A manufacturing subcontractor in the defense industry has become the latest victim of hackers, Emsisoft, a cybersecurity and anti-malware company, told Fifth Domain.
- Lockheed Martin, General Dynamics, Boeing and SpaceX are among dozens of companies named as victims of compromised data, accessed through the hacking of Visser Precision LLC, a Colorado-based aerospace, automotive and industrial parts manufacturer.
- DoppelPaymer, a ransomware group, perpetrated the hack, according to Brett Callow, a threat analyst with Emsisoft.”
- …”Hacker groups — such as Maze, which previously released veterans’ sensitive information online — have targeted various government entities, law firms and businesses in the last year, as reported by Military Times, a sister publication of Fifth Domain.
- Standard to other ransomware attacks, the hackers appear to have gained access to Visser Precision’s system, exfiltrating data before demanding payment to prevent a wider release.”



Industry

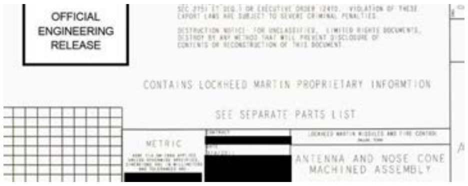
A hacker group says it has major defense companies’ data

Dylan Gresik

date_range 1 day ago

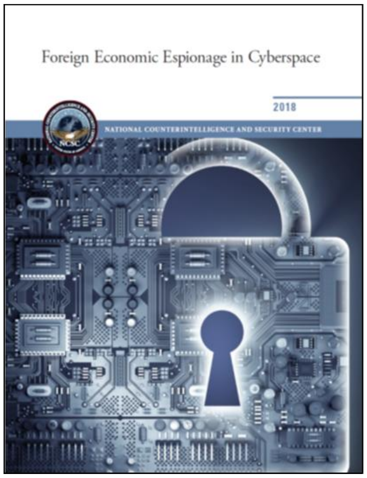
DoppelPaymer, a ransomware group, claims to have accessed sensitive data from major defense industry companies through the hacking of Visser Precision LLC, a Colorado-based aerospace, automotive and industrial parts manufacturer. (Zephyr18/Getty Images)

https://www.fifthdomain.com/2020/03/02/a-hacker-group-says-it-has-major-defense-companies-data/



OFFICIAL
ENGINEERING
RELEASE
SEC 2751 ET SEQ.) OR EXECUTIVE ORDER 12470. VIOLATION OF THESE EXPORT LAWS ARE SUBJECT TO SEVERE CRIMINAL PENALTIES.
DESTRUCTION NOTICE: FOR UNCLASSIFIED, LIMITED RIGHTS DOCUMENTS, DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THIS DOCUMENT.
CONTAINS LOCKHEED MARTIN PROPRIETARY INFORMTION
SEE SEPARATE PARTS LIST
METRIC
CONTRACT
[redacted]
[redacted]
[redacted]
LOCKHEED MARTIN MISSILES AND FIRE CONTROL
ANTENNA AND NOSE CONE MACHINED ASSEMBLY

Cyber Espionage


Foreign Economic Espionage in Cyberspace
2018
NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

“Cloud networks and IoT infrastructure are rapidly expanding the global online operational space. Threat actors have already demonstrated how cloud can be used as a platform for cyber exploitation. As IoT and AI applications expand to empower everything from “smart homes” to “smart cities”, billions of potentially unsecured network nodes will create an incalculably larger exploitation space for cyber threat actors.” (p. 4)

Observations

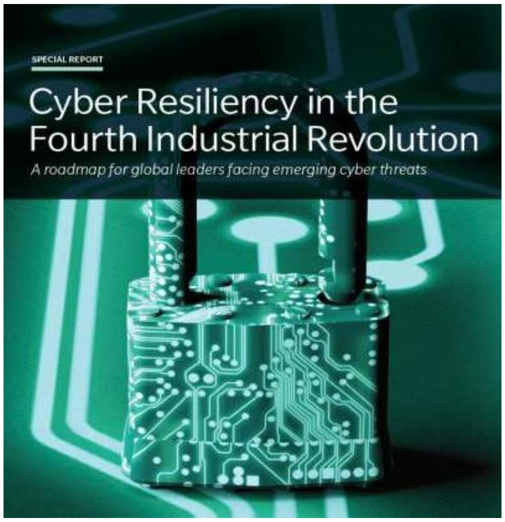
DoD program offices seem to have problems with:

- Adapting overarching cybersecurity guidance to effective systems security requirements -- current guidance is at an outcome level;
- Translating enterprise cyber intelligence and warning into an understanding of cybersecurity risk for probability and impact to their system;
- Realizing if industry cybersecurity threats apply in a consistent manner;
- Applying risk mitigation strategies for their systems, especially system vulnerabilities in potential hostile operational environments;
- Accepting risk due to an inability to change cybersecurity design decisions due to their acquisition lifecycle stage or being legacy; and
- Helping Resource Sponsors, Milestone Decision Authority, and Approving Official to understand consequences of cyber vulnerabilities for funding, personnel, & schedule

Assumptions

- Cybersecurity is a decaying function - static cyber policy translates into a reduced security posture everyday
- NO SYSTEM is without malware - every system has an inherent vulnerability that is just waiting to be exploited
- Seemingly secure systems fail to acknowledge possible exploitation by a higher level of threat
- Cybersecurity Policy stands at the Outcome level; Acquisition below the outcome level is subjective - i.e "Design for the Fight"
- Most programs struggle with “adequate security” - most operate under a false sense of security until they discover they don't
- DoD may not be proactive enough to exploit its own systems (e.g. Netflix’s Chaos Monkey/Simian Army)

What’s New in Cybersecurity?



SPECIAL REPORT

Cyber Resiliency in the Fourth Industrial Revolution

A roadmap for global leaders facing emerging cyber threats

2020 Cyberthreat Defense Report

"IT security teams can use the data, analyses, and findings to shape answers to many important questions, such as:

- Where do we have gaps in our cyberthreat defenses relative to other organizations?
- Have we fallen behind in our defensive strategy to the point that our organization is now the "low-hanging fruit" (i.e., likely to be targeted more often due to its relative weaknesses)?
- Are we on track with both our approach and progress in continuing to address traditional areas of concern, while also tackling the challenges of emerging threats?
- How does our level of spending on IT security compare to that of other organizations?
- How are other IT security practitioners thinking differently about cyberthreats and their defenses, and should we adjust our perspective and plans to account for these differences?" (p. 4)

The Road Ahead: Cybersecurity in 2020 and Beyond

- The Cloud Has Changed Security
  - Customers retain responsibility of ensuring they operate the cloud offering that maintains their own security requirements, follow all best practices, and address applicable regulatory compliance/audit requirements
- Proof of Compliance
  - 2020 will require providers to offer more proof of compliance to industry regulations and customer requirements, with clear ways for customers to validate that vendors are doing what they say they are doing
- Security Hygiene
  - As organizations move development environments outside their perimeter, they must be diligent in ensuring they protect their development and staging environments at the same level as their operation environments, and should never keep them available longer than required to perform necessary tasks
- Staffing Outside the Box
  - Security leaders need to reconsider our notions of what makes a great security candidate by looking beyond the typical security certifications
- Mind the Supply Chain
  - The lack of visibility into the details of an offering can lead to unexpected exposures if it was relied on to perform a specific security function or if it grants a previously unavailable or undocumented capability or data access if it was compromised

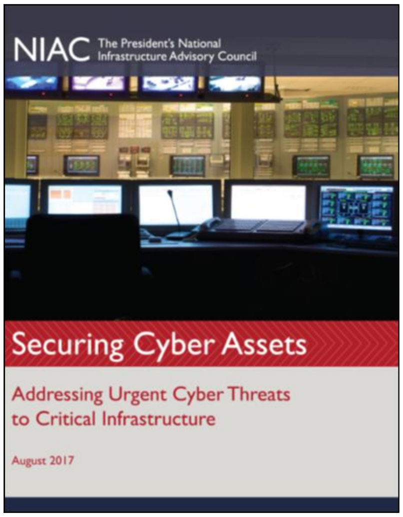
A Cyber Thread Runs Through Government Future Assessments

The future of U.S. technology, if the federal government has its way, likely will be cyber-heavy with innovative breakthroughs erupting from several areas, according to the office charged by Congress with assessing things to come. These areas include seemingly mundane concerns such as telecommunications and digital ledger capabilities, along with more advanced issues such as artificial intelligence and quantum systems.

Many of these disruptive technologies have policy ramifications either in their development or their implementation. The federal government must consider aspects such as regulatory issues, privacy, economic competitiveness and security requirements.

- The GAO's top scientific priority as directed by Congress is artificial intelligence (AI), Persons says.
- Another high priority is 5G technology.
- Blockchain is another key technology focus area, and the GAO is taking its three-level approach to the capability's future

Best Practices



NIAC The President's National Infrastructure Advisory Council

Securing Cyber Assets

Addressing Urgent Cyber Threats to Critical Infrastructure

August 2017

1. "Establish **SEPARATE, SECURE COMMUNICATIONS NETWORKS** specifically designated for the most critical cyber networks, including "dark fiber" networks for critical control system traffic and reserved spectrum for backup communications during emergencies." **(Dark fiber** refers to unused fiber-optic cable)
2. **"FACILITATE A PRIVATE-SECTOR-LED PILOT OF MACHINE-TO-MACHINE INFORMATION SHARING TECHNOLOGIES**, led by the Electricity and Financial Services Sectors, to test public-private and company-to-company information sharing of cyber threats at network speed.**"**
3. "Identify best-in-class **SCANNING TOOLS AND ASSESSMENT PRACTICES**, and work with owners and operators of the most critical networks to scan and sanitize their systems on a voluntary basis**."** (pp. 7-10)

Supply Chain Risk Management: A Growing Concern

Deliver Uncompromised

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

Chris Nissen, John Gronager, Ph.D., Robert Metzger, J.D., Harvey Rishikof, J.D.

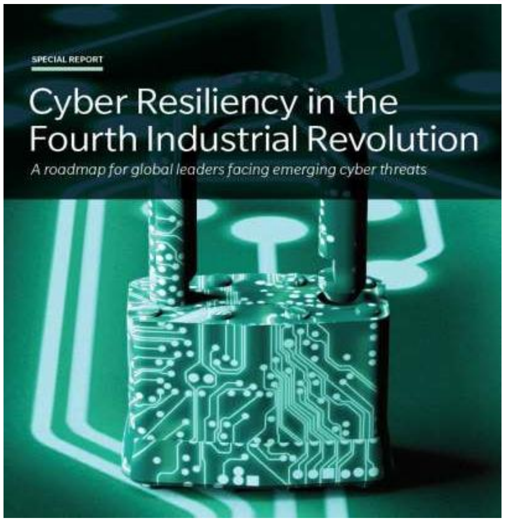
MITRE

- Identify, protect, detect, respond to, and recover from network and supply chain threats
- Increase coordination with IC, DHS, and civilian agencies
- Improved relations with contractors; changes to acquisition strategy and practice (require Maturity Certifications)
- View risk-based security as a profit center for capturing new business, not as a harmful expense to the bottom line
- DoD cannot control all the actions of its numerous information system and supply chain participants
- DoD to use its purchasing power and regulatory authority to move companies to work with DoD to enhance security through addressing threat, vulnerabilities, and consequences of its capabilities and adapt to dynamic, constantly changing threats
- Fundamental SCRM Instruction based on DoDI 5200.44, “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)”

28

28

Summary



SPECIAL REPORT

Cyber Resiliency in the Fourth Industrial Revolution

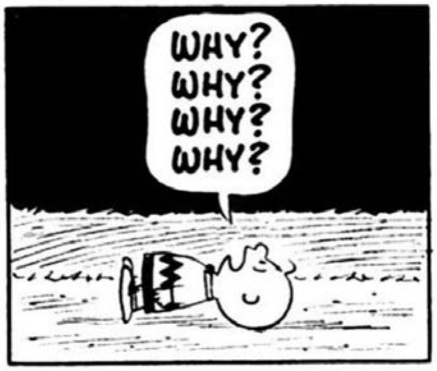
A roadmap for global leaders facing emerging cyber threats

29

29

Today's Discussion

- Why the Need for Cybersecurity
- How and Why Threats are Impacting US Manufacturing
- What is New in Cybersecurity



30

30

Box of Chocolates

Cybersecurity is like a box of chocolates ….

You never know what you are going to get

31

31

Defense Arms Parade; "Cyberwarriors"

SACK
HACKERS

Let’s Peel Back the Onion

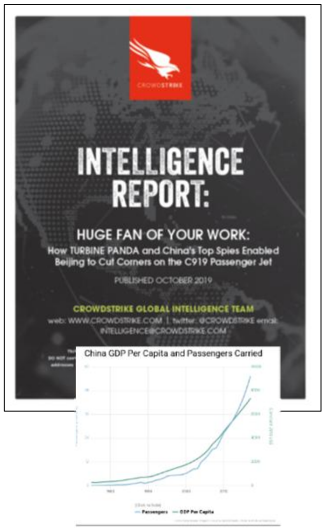
What’s important now …

Supply Chain - **Defensible Methods**

- Program Protection Plan (PPP)
- Supply Chain Risk Management (SCRM)
- Software Assurance (SwA)

Are we Serious About This Change?

15 Oct 2019 Crowdstrike Intel Report



CROWDSTRIKE

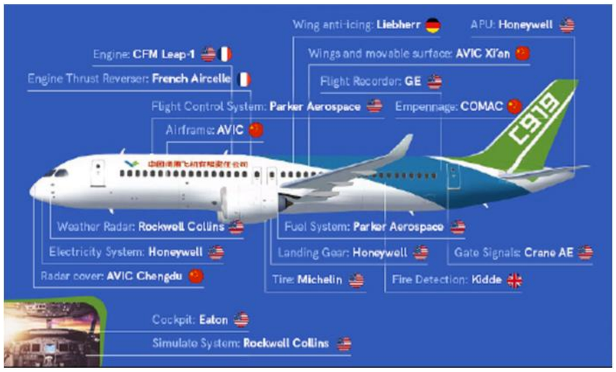
INTELLIGENCE REPORT:

HUGE FAN OF YOUR WORK:
How TURBINE PANDA and China's Top Spies Enabled Beijing to Cut Corners on the C919 Passenger Jet

PUBLISHED OCTOBER 2019

CROWDSTRIKE GLOBAL INTELLIGENCE TEAM
web: WWW.CROWDSTRIKE.COM | twitter: @CROWDSTRIKE email: INTELLIGENCE@CROWDSTRIKE.COM

China GDP Per Capita and Passengers Carried


Wing anti-icing: Liebherr
APU: Honeywell
Engine: CFM Leap-1
Wings and movable surface: AVIC Xi'an
Engine Thrust Reverser: French Aircelle
Flight Recorder: GE
Flight Control System: Parker Aerospace
Empennage: COMAC
Airframe: AVIC
C919
Weather Radar: Rockwell Collins
Fuel System: Parker Aerospace
Electricity System: Honeywell
Landing Gear: Honeywell
Gate Signals: Crane AE
Radar cover: AVIC Chengdu
Tire: Michelin
Fire Detection: Kidde
Cockpit: Eaton
Simulato System: Rockwell Collins

"…we take a look at how Beijing used a mixture of cyber actors sourced from China's underground hacking scene, Ministry of State Security officers, company insiders, and state directives to fill key technology and intelligence gaps in a bid to bolster dual-use turbine engines … to compete against western aerospace firms" (p. 1)

For additional questions, please contact Chris Newborn at chris.newborn@dau.edu or 619-370-3076