

Total Defense High Tech

Drs. Ir. Aernout Reijmer
Senior Director ASML Security
SMCC Governing Council

November 7, 2024
Munich

The world is changing - we need to change with it

Canon confirms August ransomware attack, notes past and current employees affected

Published Nov 30, 2020 | Gannon Burgett

Benchmark Electronics (BHE) reports systems were incident recently affected by ransomware

Article Related SEC Filings (2) Stock Quotes (1) Comments (0)

November 6, 2019 6:57 AM EST

Tweet Share E-mail

Semiconductor giant SK Hynix silent on ransomware attack

By Juha Saarinen, TNews Aug 20 2020 11:57AM
Supplies memory modules to Apple and PC makers.

Toshiba victim of Ransomware - halts production of NAND Flash (updated)

by Hilbert Hagedoom on: 10/17/2017 08:09 AM | source: | 14 comment(s)



Toshiba has suspended NAND flash production in its Japan facilities for a few weeks due to ransomware attacks on its computer network, according to sources at channel distributors. The incident could tighten global NAND flash supply.

Intel leak: 20GB of source code, internal docs from alleged breach

By Ionut Ilascu

August 6, 2020 04:45 PM 1



Classified and confidential documents from U.S. chipmaker Intel, allegedly resulting from a breach, have been uploaded earlier today to a public file sharing service.

Ransomware attack: Maastricht University pays out \$220,000 to cybercrooks

Adam Bannister 07 February 2020 at 16:05 UTC
Updated: 11 May 2020 at 08:17 UTC

Ransomware Netherlands Cybercrime

Tweet WhatsApp Facebook Reddit LinkedIn Email

Dutch institution regrets striking 'devil's bargain' but said it had to put staff and students first

Compal, the second-largest laptop manufacturer in the world, hit by ransomware

Compal factories build laptops for Apple, Acer, Lenovo, Dell, Toshiba, HP, and Fujitsu.

By Catalin Cimpanu for Zero Day | November 9, 2020 -- 12:49 GMT (12:49 GMT) | Topic: Security

The NSA Warns That Russia Is Attacking Remote Work Platforms

A vulnerability in VMware has prompted a warning that companies—and government agencies—need to patch as soon as possible.

Ransomware gangs are now cold-calling victims if they restore from backups without paying

Tactic used since August by ransomware gangs like Sekhmet, Maze, Conti, and Ryuk.

Foxconn Ransomware Attack Reportedly Damages Servers, Backups

The ransomware attack was carried out by DoppelPaymer, who's demanding \$34.7 million in Bitcoin and leaked generic Foxconn business documents and reports Monday, according to BleepingComputer.

By Michael Novinson

December 07, 2020, 03:25 PM EST

MIVD onthult werkwijze Chinese spionage in Nederland

Nieuwsbericht | 06-02-2024 | 15:33

De Militaire Inlichtingen- en Veiligheidsdienst (MIVD) heeft Chinese cyberspionage in Nederland blootgelegd. De dienst ontdekte geavanceerde Chinese malware die dit mogelijk maakt. Een Chinese statelijke actor is hiervoor verantwoordelijk. Dit stelt de MIVD op basis van eigen inlichtingen vast.



Ransomware warning: Now attacks are stealing data as well as encrypting it

Altran hit by a Cyber Attack and Ransomware is suspect

Posted By: Naamen Gaur

Our Business Ecosystem is increasingly at risk

Multiple mega-trends affecting society are going in the wrong direction



ST1. The number of new vulnerabilities and zero-days per day continues to steeply increase



ST2. Cybercrime, i.e. ransomware, will increase 2x by 2031. Now the 3rd world economy, growing 15% YoY.



ST3. Geopolitical pressure will continue to intensify, leading to more attempts in IP theft.

But the supply chain focuses on the Ransomware Risk. The threat of war (cyber/kinetic) is increasing.



ST4. Digitalization of our society / economy continues. GenAI, PQC are disruptive technologies.

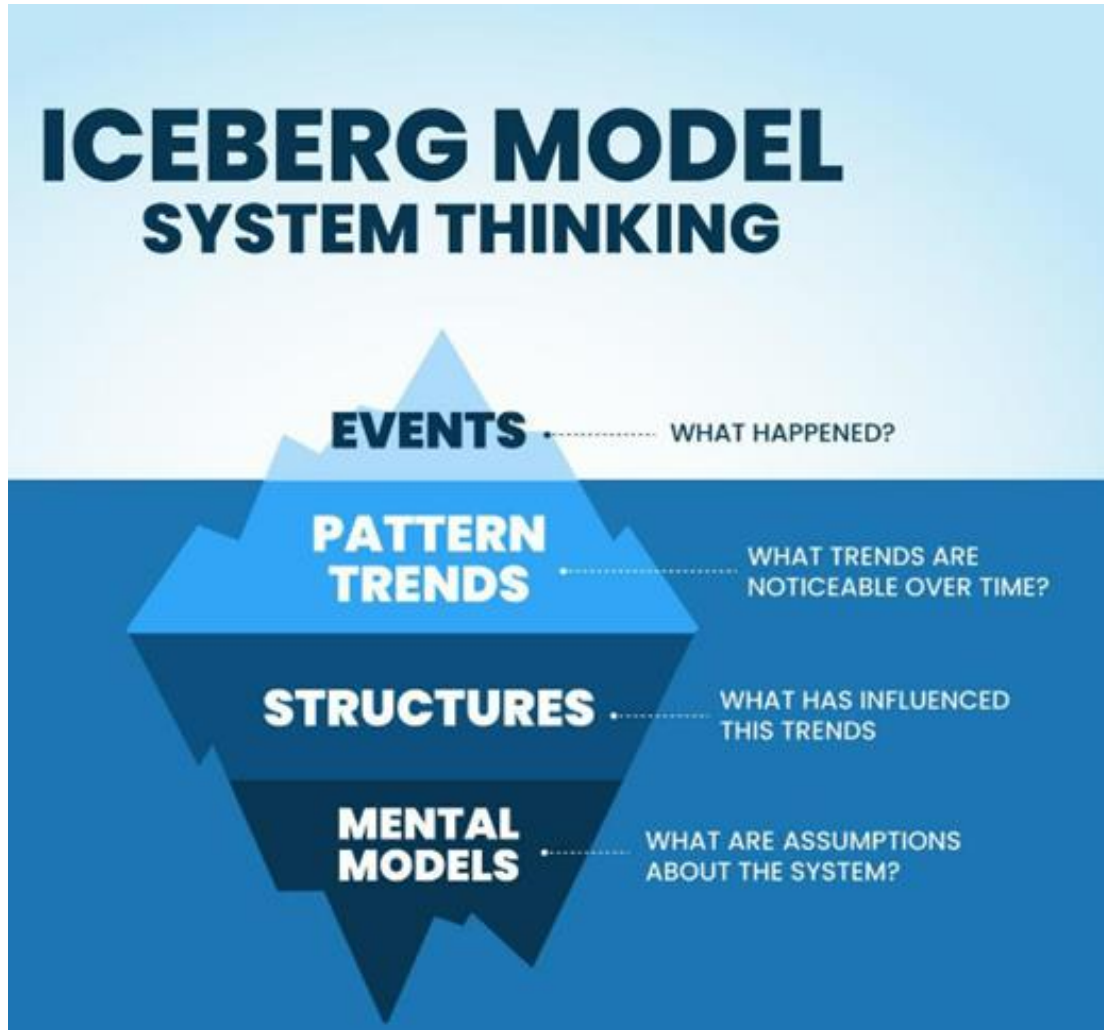


ST5. Yearly new workforce FTE joining the cyber war (in NL) is in the 100s, when 1000s are needed.`



ST6. More Legislations and Regulations, in more and more countries. Not always in line with each other.

The trends are moving in the wrong direction for our security



- Ransomware. The costs of cyber crime are high
- IP theft
- Upcoming laws and legislations such as NIS2 and CRA
- Digitalization and cloud; PQC is heading our direction
- Increase in Cyber Incidents
- Steeply increase in the number of new vulnerabilities
- Yearly new workforce joining the cyber war (in NL) is in the 100s, when 1000s are needed.
- Who is responsible for security; what is the legal framework
- Who should do what in the field of Cyber Security?
- How much are we willing to pay to become 'secure'?
- How much risk are we willing to take?
- What is the role of the government and business?
- Big helps small; but how often?

"If you do what you always did, you're going to get what you always got"

A large shark is breaching the water surface, its mouth wide open, revealing sharp teeth and a bloody interior. The water is splashing around the shark's head.

**if we don't change
anything, we will have a
big problem**

Towards a knowledge-intensive government: Use and dissipate the existing cyber knowledge and insights in the business community

- Cyber Weather Report / Alert regarding vulnerabilities
- Cyber Threat Intel on threats
- Central library with Best Practices and action perspective, how do you get 'in control'

We need less fragmentation, set stronger direction/agenda, coordination and execution power by the government on this – not new regulation though..!



We need to organize and boost knowledge sharing through Public Private Partnerships

- Overcome the incentive of internal focus
- Big helps Small
- Strengthen sectoral/regional cyber resilience initiatives
- Practice with each other: know where to find each other in advance; improve crisis management together



Cyber is a knowledge and intelligence war between experts

Provide budget for a future shaped by Cyber Experts

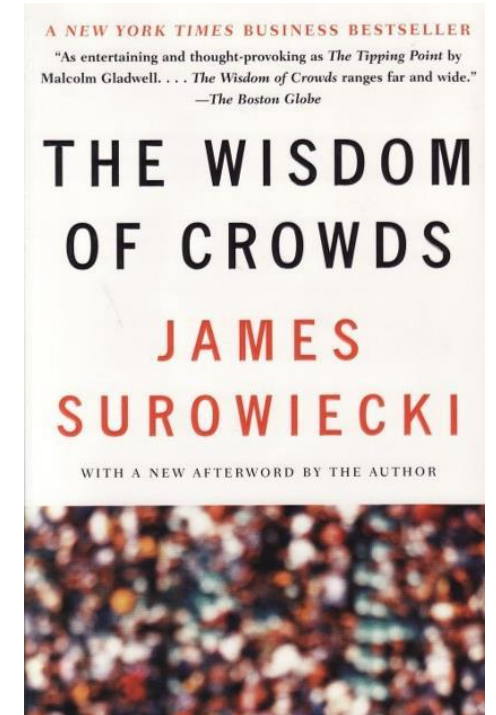
- More educational programs should be able to start
- Together with Universities / HBO / MBO
- Facilitate Internships for students and job rotation with government
- Not just Master students, also provide practical training
- Business and government should jointly offer an attractive career path to young people choosing their future.



The Wisdom of the Crowd is the foundation of our Collective Defense.



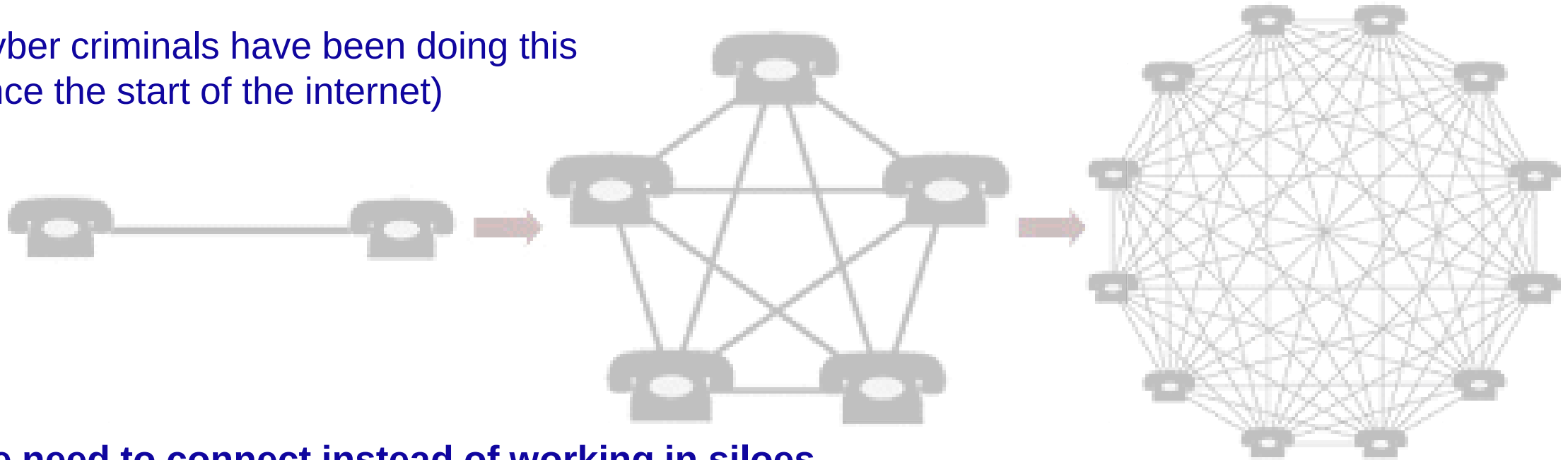
With the Government as an independent authority towards the expertise that is present in the business community the insights can be put to greater use towards the ecosystem as there is no attribution.



Metcalfe's Law

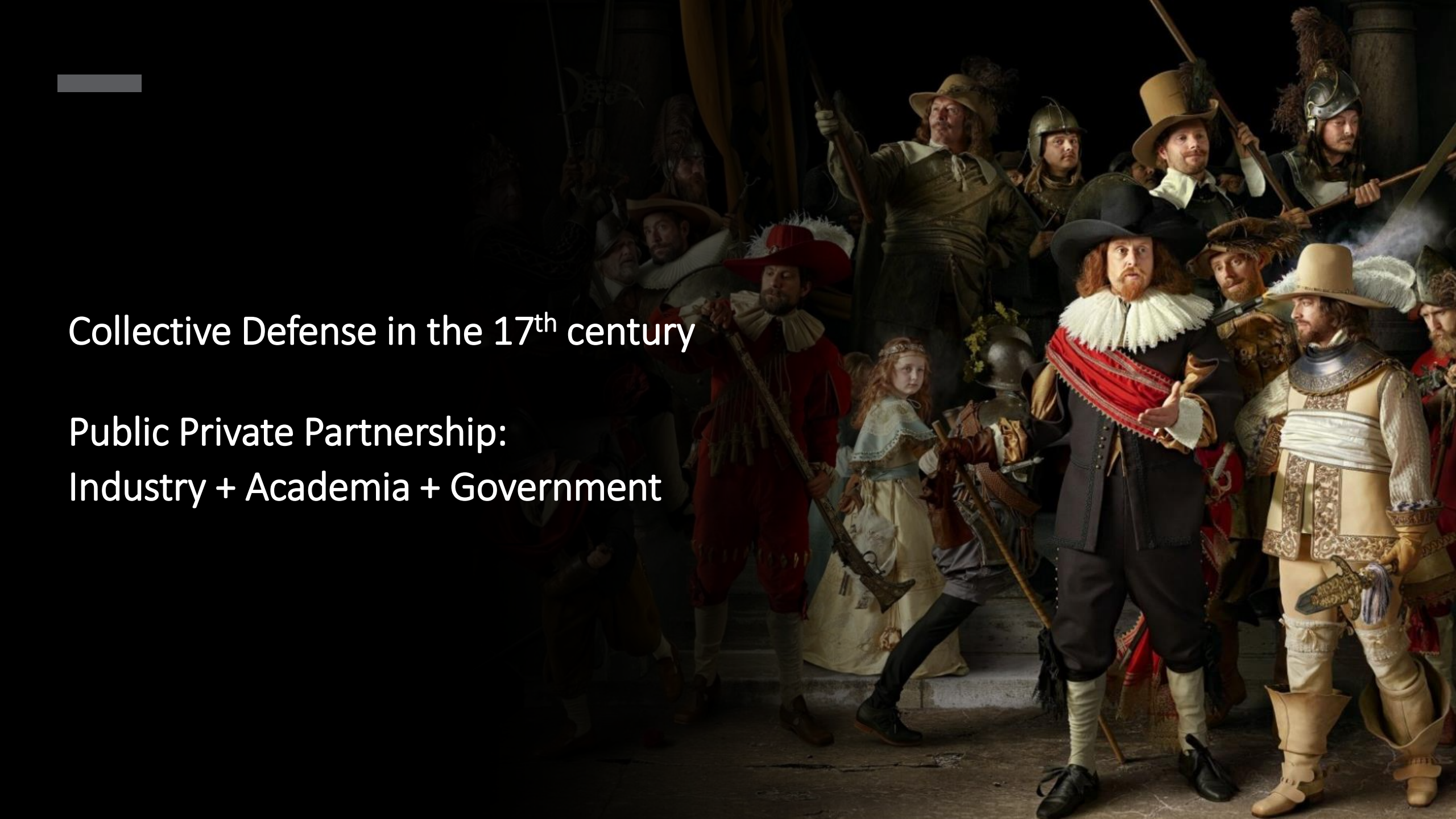
'The value of a network increases exponentially compared to the number of new nodes in the network'

(cyber criminals have been doing this since the start of the internet)



We need to connect instead of working in siloes.

Building, uniting and making knowledge networks efficient has major advantages; As well as taking criminal networks offline



Collective Defense in the 17th century

Public Private Partnership:
Industry + Academia + Government

ASML

2022 Market Data Estimates Sources: SEMI, IC Insights and TechInsights



SMCC Governance Structure

Governing Council

Strengthen cyber resilience and protection of the global semiconductor supply chain against evolving threats



Kannan Perumal
VP & Chief Information Security Officer
Applied Materials





Aernout Reijmer
Chief External Security Officer
ASML





Wes Sparks
Director, Supply Chain – Factory Automation, AI, & Cybersecurity
Intel





James Tu
Head of Corporate Information Security,
TSMC





Doug Suerich
Director of Marketing
PEER Group



Steering Committee

Develop a standards-based, industry-wide approach to improve cybersecurity and accelerate implementation of actionable solutions

	WG1: Factory Cybersecurity Implementation	WG2: Compliance Readiness	WG3: Supply Chain Cybersecurity	WG4: Standards & Regulations	WG5: Threat Sharing	WG6: CyS Pre-Standards Engineering	WG7: Outreach, Comms & Events
WG Chairs	 Brian Korn Staff Technologist Intel Foundry 	 Dave Dunne Manager, Product Security Engineer 	 Eiji Hagio Vice President Information Security 	 Jennifer Lynn CISO Cyber Defense Leader - IBM Semi 	 Bill Higgs Senior Security Officer External Affairs 	 Leon Chang Deputy Director 	 Mayura Padmanabhan Technical Project Mgr 
WG Vice-Chairs	 Leon Chang Deputy Director 	 Leon Chang Deputy Director 	 Lori G. Kessler Sr. Program Director, Info Security & Risk Mgt 	 Rajesh Potturi Sr. Director Information Security & Risk Mgt 	 Jennifer Lynn CISO Cyber Defense Leader - IBM Semi 	 Ryan Bond Software Application Architect 	 Quentin Ellis Marketing Manager 
	 Dave Dunne Manager, Product Security Engineer 	 Brian Korn Staff Technologist Intel Foundry 	 Bill Higgs Senior Security Officer External Affairs 	 Wilko Baks Manager Product Security 	 Chet Borg Director of IT 	 Albert Fuchigami Senior Standards Specialist 	 Open Position

WG1	WG2	WG3	WG4	WG5	WG6	WG7
Factory Cybersecurity Implementation	Compliance Readiness	Supply Chain Cybersecurity	Standards & Regulations	Threat Sharing	Pre-Standards Engineering	Outreach, Comms & Events
Operationalize cybersecurity specs for factory tools & ID roadblocks Starting with SEMI E187	Implementation of methods to ensure tools are compliant with SEMI standards	Establish methods for ecosystem (supply chain) security implementation & management	Develop strategy for pending legislation & global standards eg. NIST CSF 2.0, EU CRA, ONCD NCS, ISA/IEC 62443	Implement methods for cyber threat intelligence sharing	Architect comprehensive strategy for new & updated SEMI standards	Execute cybersecurity education and awareness campaign for semiconductor manufacturing & supply chain

As of 5/8/24

SMCC Member Companies- 60 and growing

Device
Makers
9



OEMs
20



Solution
Providers
21



Govt &
NGOs
9
ASML



Learn from each other, don't compete on Cybersecurity

We're in this cyber arms race together

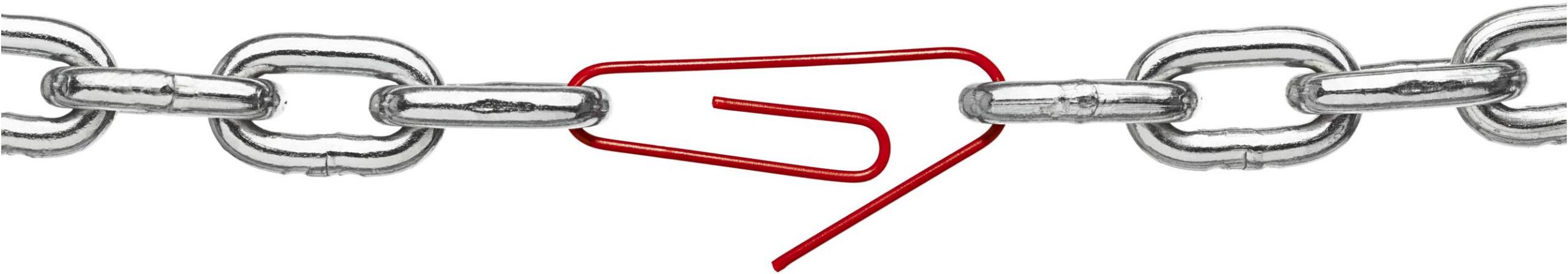
Don't reinvent the wheel
Don't work in siloes



Benefit and Learn from each other!



We are all connected



Join the Semiconductor Manufacturing Cybersecurity Consortium!