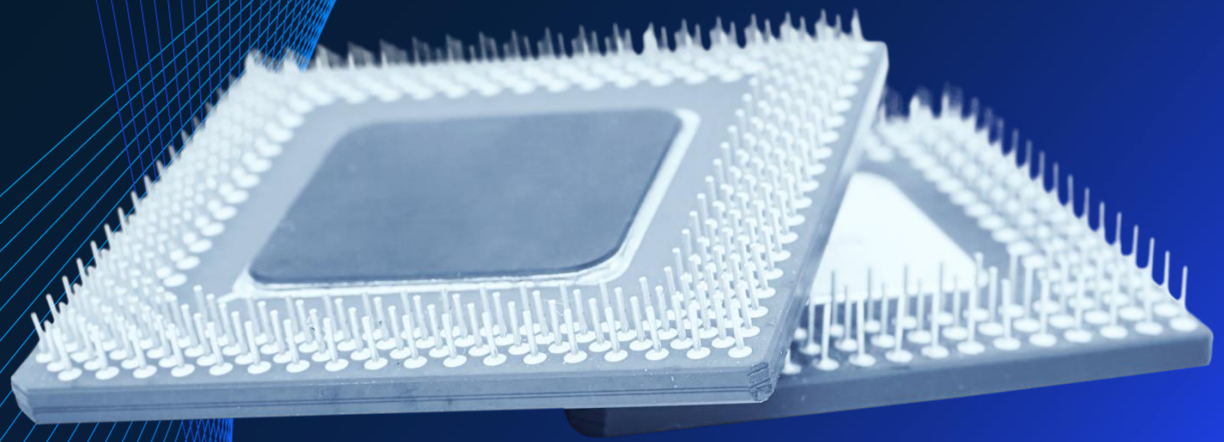
McKinsey & Company

Tech brief: Cyber-security

February 2020



Cybersecurity is a major issue, and threats are constantly growing

What everybody knows

Relentless and sophisticated attackers

More assets stored and processes executed in digital form

Increasing regulatory scrutiny

$150 million
2020 cost of data breach

36%
ransomware attacks increase in 2017

175+
confirmed breaches per day

101
average days between breach and discovery

50%
percent of websites with web application vulnerabilities

$3 trillion
2019 cybercrime costs

What not everyone realizes

Attackers have institutionalized cybercrime

- Leverage cutting-edge malware stolen from US intel community
- Build data warehouses of personal information gleaned from hundreds of attacks
- Set up outsourced call centers to support social engineering

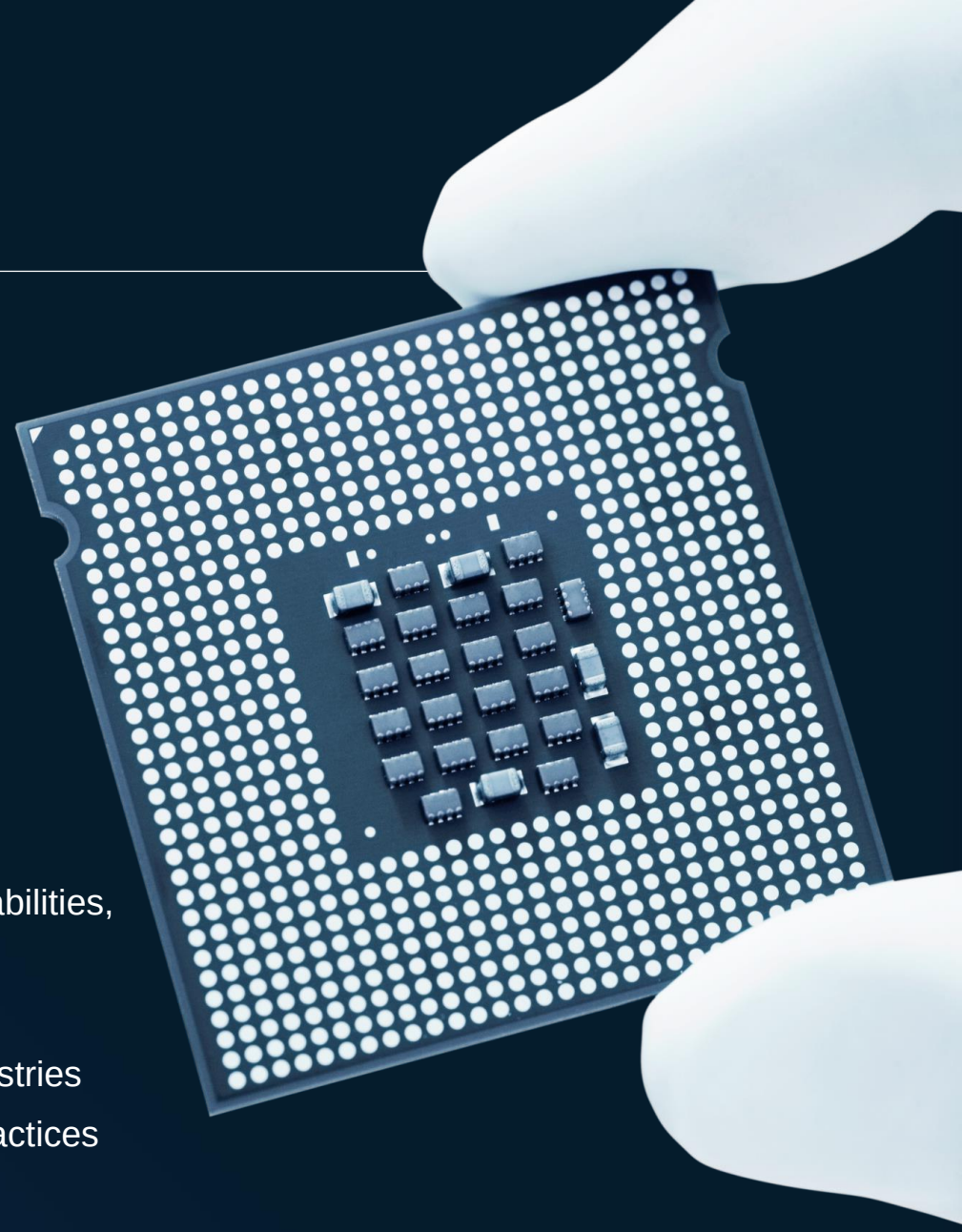
As states militarize cyberspace, private companies become collateral damage

- Cyber-espionage (e.g., Marriott)
- Destructive cyber-warfare (e.g., notPetya)

Customers placing increasing pressures on vendors to demonstrate cybersecurity capabilities, shaping buying decisions and slowing contracting

Digital business strategies and technology vastly increasing risk

- IoT expands risk of product compromises and business disruption in a broad of industries
- Agile, cloud, RPA, DevOps and analytics disrupt existing cyber architectures and practices



Security is imperative, especially given that cyber threats on satellites are on the rise

Many cyber attacks have occurred on satellites …

2007

June, October 2008

NASA-managed Terra AM-1 earth observation satellite suffered interference for 2 mins in June, 9 mins in October 2008

2010

March 2011

Theft of unencrypted NASA notebook computer resulted in loss of algorithms used to command and control the International Space Station (ISS)

November 2011

Two satellites belonging to NASA, USGS suffered interference (espionage motive)

2013

March 2012

BBC reported a "sophisticated cyber-attack" which coincided with efforts to jam two BBC satellite feeds to Iran

September 2014

NOAA's Satellite Data Information System taken offline, resulting to no weather data across the globe for 48 hours

2016

September 2015

Turla APT hijacked satellite to steal data from thousands of hacked computers in US and Europe

June 2017

US Maritime Administration reported the first GPS spoofing attack against over 20 ships in the Black Sea

August 2017

French Defense head charged a foreign government with one of the first ever cases of space espionage

2019

June 2018

Event of cyber espionage to collect data from satellite, telecom, and defense organizations in US and Southeast Asia reported

… and experts believe that there will be more

"Cyber experts say threats to satellites are legion"

- SpaceNews (2017)

"Danger from cyber-attacks is only increasing, and the [satellite] industry is a likely target"

- Via Satellite (2018)

"Our satellites are prime targets for a cyberattack. And things could get worse"

- The Washington Post (2019)

"Cybersecurity challenges will only become more substantial … space assets are [the] weakest link"

- Harvard's Gregory Falco (2018)

"Cyber breaches abound in 2019 […] more cyber attacks on satellite"

- TechCrunch (2018)

"… anticipate major attacks on satellite systems as a new form of nation-state warfare"

- Forbes (2018)

Source: Center for Strategic and International Studies, Council on Foreign Relations, press search

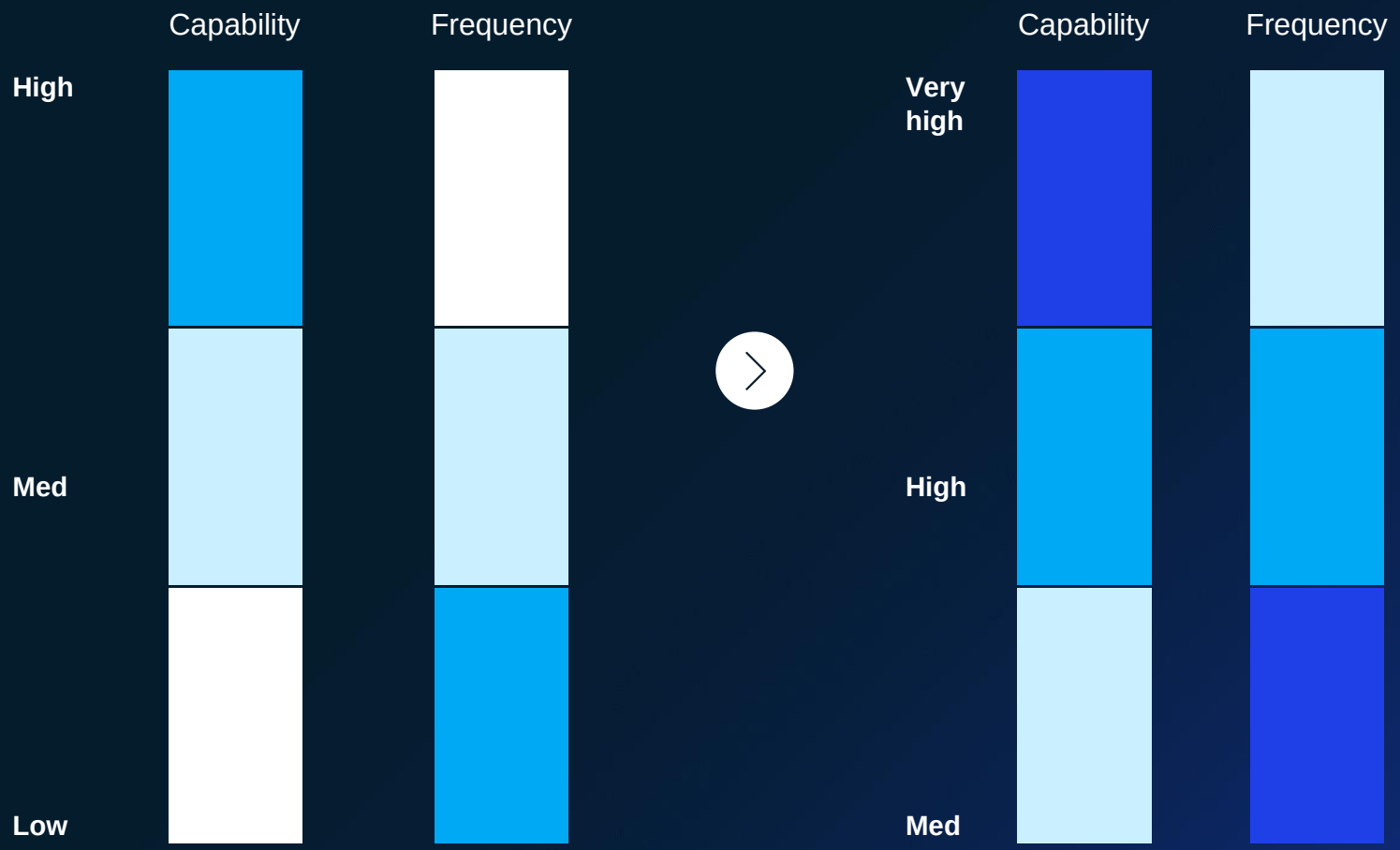
The landscape of cyber threats is growing more complex, with attackers improving their craft, leveraging better tools, and accessing more data

Yesterday

Today

Threat actor

- Nation-state
- Organized crime
- Hacktivist groups
- Competitors
- Insider threat
- Opportunists/ script kiddies



Security aspect need to be considered across supply chain

Supply chain is one weak link in cyber security

NIST National Institute of Standards and Technology

80%

information breaches **originate in the supply chain**

45%

cyber breaches were attributed to **past partners**

72%

companies **do not have full visibility** into their chains

59%

companies **do not process for assessing cyber security of 3rd party providers**

"In the satellite industry, the supply chain could very well be the weak link"

— Via Satellite (2018)

Via Satellite

Source: NIST (2016), Press Search

Many satellite providers look for in-house security teams, but talent is scarce

Plan to initially setup a ~10 people in-house security team …

Will engage **external expert** for initial team setup

Chief Information Security Officer

Experts e.g., network security, IRT (5-6 people)

Database maintenance specialists (2-3 people)

Security Officer dedicated to raise awareness on security (1 person)

… yet as talent may be scarce, may need to cultivate it early

Globally

2 million

shortage of cyber security professionals by 2019

53%

organizations experience delays as long as 6 months to find candidates

In country

Minimal cybersecurity educational program exist

Major universities offer courses, but **no accreditation** exist

Graduates' **skill sets often fall short** of what the industry requires

Source: ISACA, World Bank, Oxford Internet Institute

In order to assure comprehensive security, satellite providers need to cover strategy, security architecture, and operating model

		Categories
Security strategy and vision		Clear **vision** from top management, emphasizing importance of information security **Information security strategy** covers all components of the **satellite's lifecycle** (i.e. design, construction, launch, operations) **Roadmap, initiatives** account for changes to satellite security technology **over time** and considers **challenges to scalability**
Security architecture	**Communication Security**	Measures are being planned/put in place to **secure communications, traffic data** across all connections, particularly: • endpoints • applications • IT infrastructure
	Physical Security	**Physical security** are being planned/put in place to protect to **ground infrastructure, equipment** that controls, regulates & monitors spacecraft (i.e. TTCM) & communication transmissions
	System Security	Measures to protect **system infrastructure**, including that of space segments, ground command centers, TTCM functions, and transmissions against external attack/interference are being planned/put in place—more particularly on (1) event & incident management; (2) vulnerability testing
Security operating model	**Policies and guidelines**	**Policies** are being planned/put in place for **users** (i.e. partner provider), **personnel** (including operational procedures), **3rd party** (i.e. vendors), ensuring **compliance with global best practices** such as NIST and **local requirements**
	Organization	Clear **organizational roles & capabilities** **Interaction/decision rights** have been thought through and match best-in-class standards **Reporting and measures** to track efficacy of cybersecurity have been discussed

Where are you in your thinking and building real capability?

McKinsey
& Company