The 2018-2019 Cybersecurity Trends

Sam Olyaei
Sr. Principal

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This presentation, including all supporting materials, is proprietary to Gartner, Inc. and/or its affiliates and is for the sole internal use of the intended recipients. Because this presentation may contain information that is confidential, proprietary or otherwise legally protected, it may not be further copied, distributed or publicly displayed without the express written permission of Gartner, Inc. or its affiliates.

Gartner®

Government Entities are on high alert!

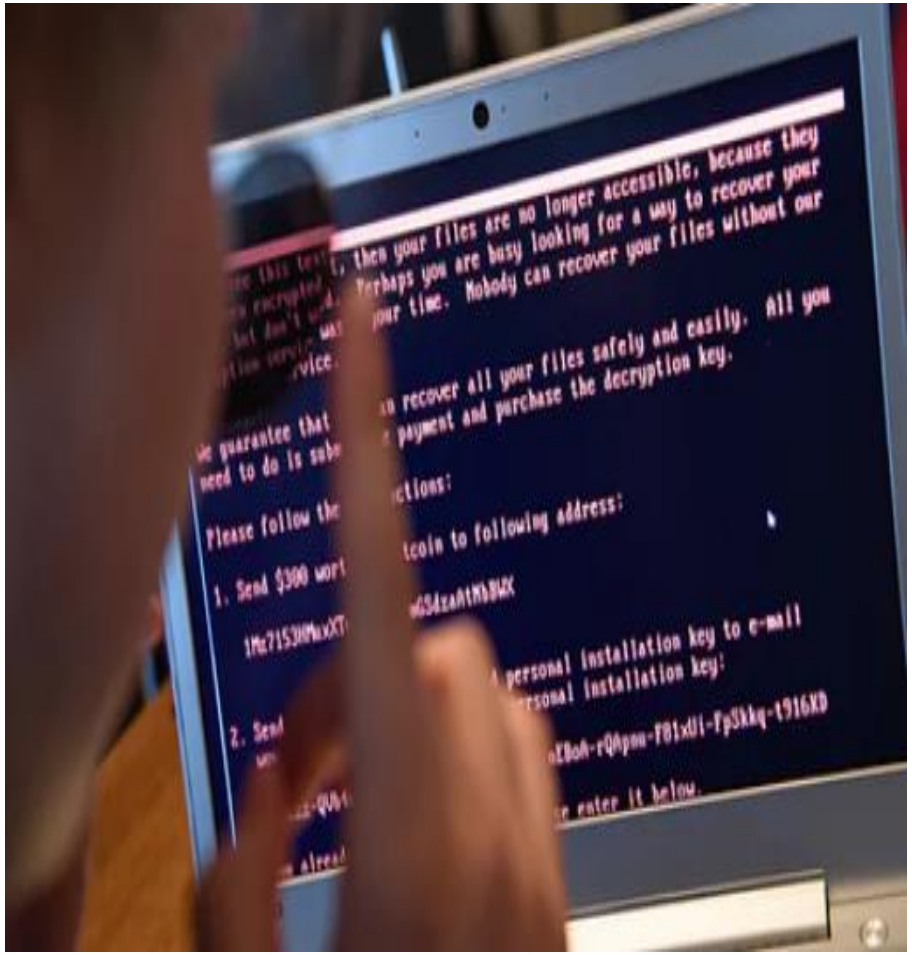
Nation state attacks unleash havoc – target is wealth and destruction!

Govt Agencies have 3-5 times the number of infected systems than the global average – lack of basic controls!

Double Digit Spend (11% growth) – BUT we are spending on the wrong things!

Organizations unable to meet regulatory requirements and deadlines

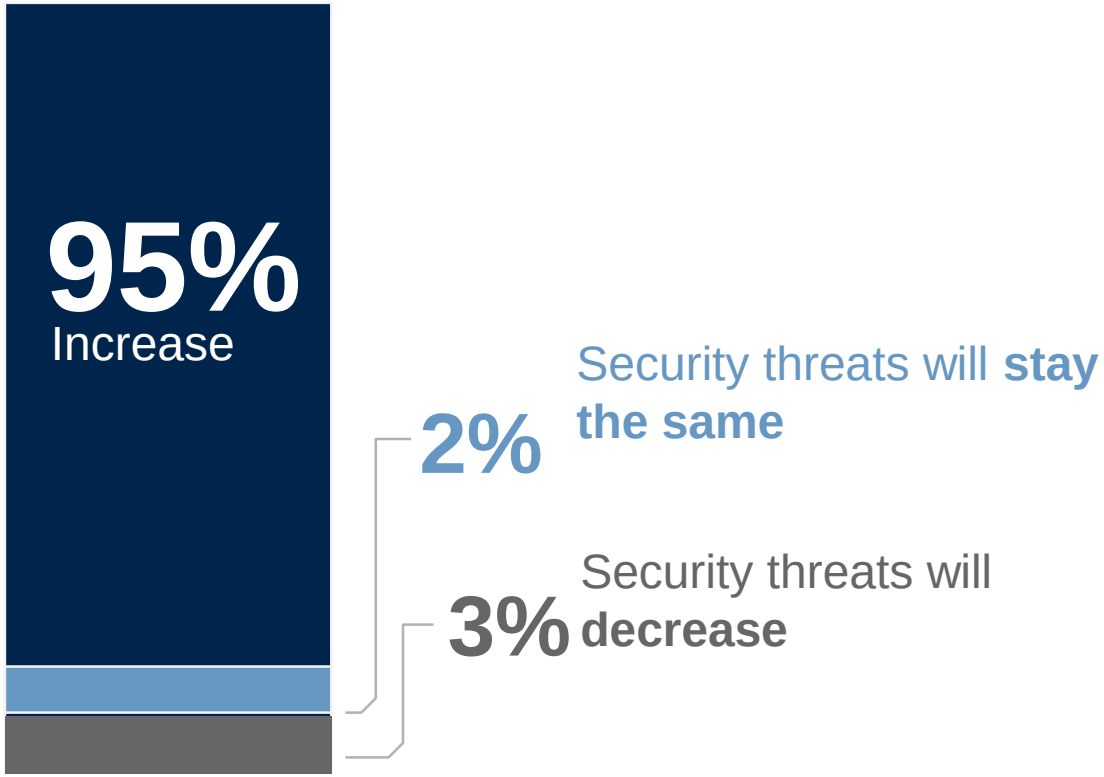
Average Maturity for Government = 2.8 vs Global Average = 3.22 (CMMI)

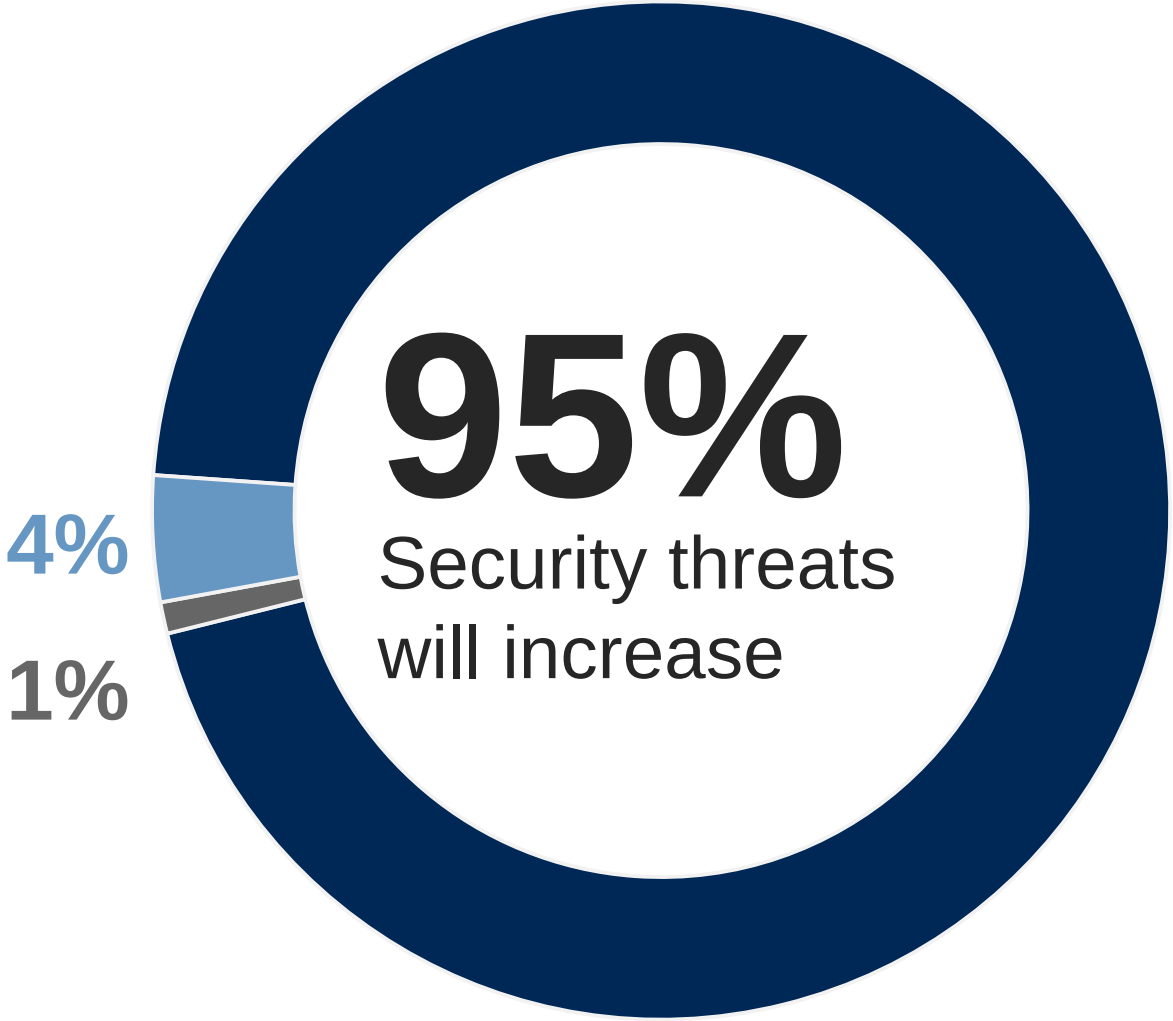


© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

It’s only getting worse..

Government CIOs





In three years, do you believe cybersecurity threats will decrease, remain the same or increase?
Total (n = 2,860); GOC (n = 58); Base: Excludes don't know.

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

Insight Report

The Global Risks Report 2018
13th Edition

IoT devices

Global population

8.4 Billion › **7.6** Billion

to accelerate and the Internet of Things is expected to expand from an estimated 8.4 billion devices in 2017 to a projected 20.4 billion in 2020.[39] What would once have been considered large-scale cyberattacks are now becoming normal. For example, in 2016, companies revealed breaches of more than 4 billion data records, more than the combined total for the previous two years.[40] Distributed denial of service (DDoS) attacks using 100 gigabits per second (Gbps) were once exceptional but have now become commonplace, jumping in frequency by 140% in 2016 alone.[41] And attackers have become more persistent—in 2017 the average DDoS target was likely to be hit 32 times over a three-month period.[42]

The financial costs of cyberattacks are rising. A 2017 study of 254 companies across seven countries put the annual cost of responding to cyberattacks at £11.7 million per company, a year-on-year increase of 27.4%.[43] The cost of cybercrime to businesses over the next five years is expected to be US$8 trillion.[44] Some of the largest costs in 2017 related to ransomware, a rapidly growing form of malware that locks targets out of their data and demands a ransom in return for restoring access. Ransomware attacks accounted for 64% of all malicious emails sent between July and September last year,[45] affecting double the number of businesses compared with 2016.[46] Notable examples included the WannaCry attack, which affected 300,000 computers across 150 countries, and Petya and NotPetya, which caused huge corporate losses: for example, Merck, FedEx and Maersk each reported third-quarter losses of around US$300 million as a result of NotPetya.[47]

Beyond its financial cost, the WannaCry attack disrupted critical and strategic infrastructure across the world, including government ministries, railways, banks, telecommunications providers, energy companies, car manufacturers and hospitals. It illustrated a growing trend of using cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning. Many of these attacks are thought to be state sponsored. WannaCry's ultimate impact was relatively low, largely because a "kill switch" was discovered, but it highlighted the vulnerability of a wide range of infrastructure organizations and installations to disruption or damage. Since the 2015 attack on Ukraine's power grid—which temporarily shut down 30 substations, interrupting power supply to 230,000 people[48]—evidence has been mounting of further attempts to target critical infrastructure. In 2016, for example, an attack on the SWIFT messaging network led to the theft of US$81 million from the central bank of Bangladesh. The European Aviation Safety Agency has stated that aviation systems are subject to an average of 1,000 attacks each month.[49] Last year saw reports of attempts to use spear-phishing attacks (stealing data or installing malware using individually targeted email scams) against companies operating nuclear power plants in the United States.[50]

Most attacks on critical and strategic systems have not succeeded—but the combination of isolated successes with a growing list of attempted attacks suggests that risks are increasing. And the world's increasing interconnectedness and pace heightens our vulnerability to attacks that cause not only isolated and temporary disruptions, but radical and irreversible systemic shocks.

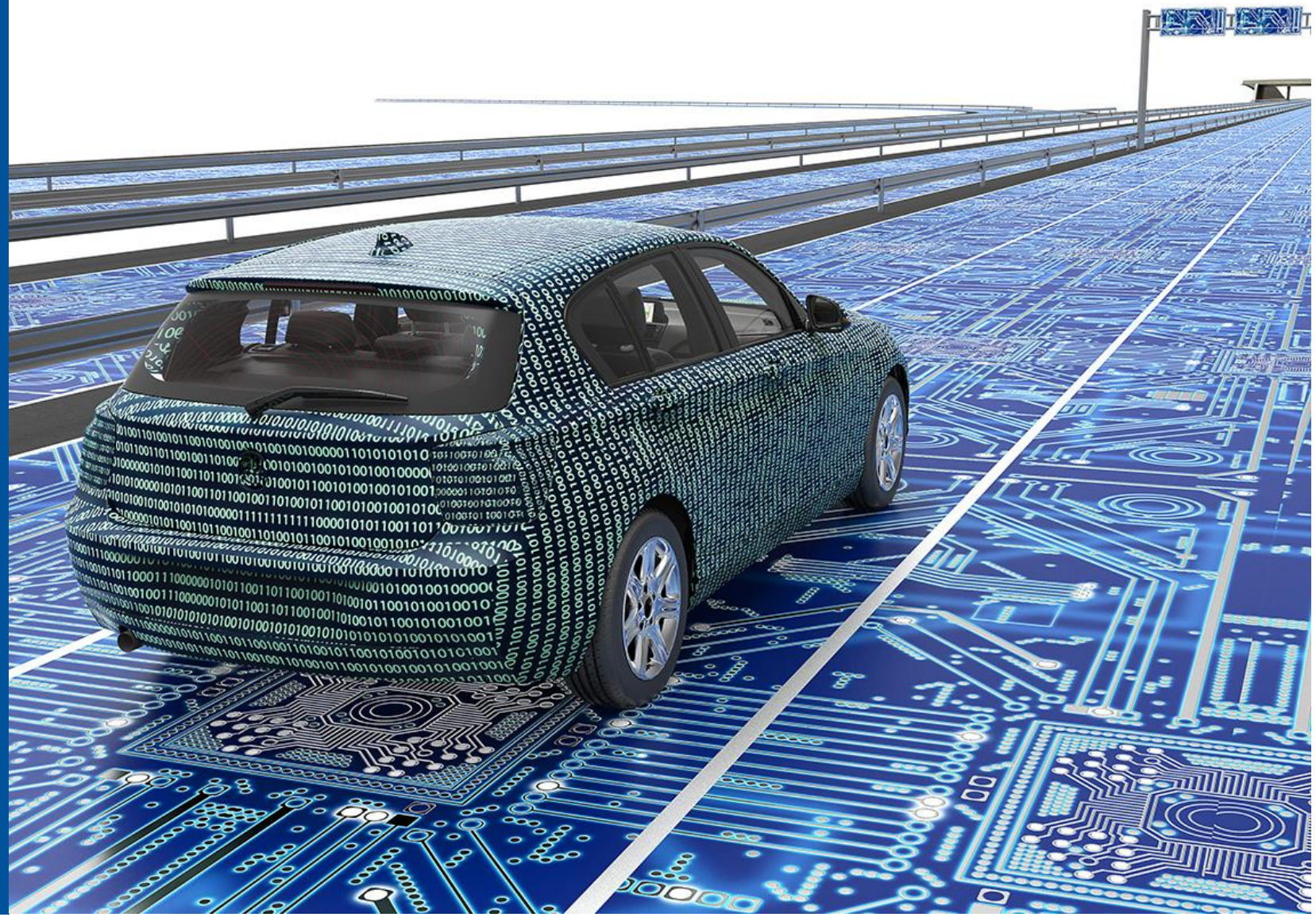
Our growing vulnerability to systemic risks

Humanity has become remarkably adept at understanding how to mitigate countless conventional risks that can be relatively easily isolated and managed with standard risk-management approaches. But we are much less competent when it comes to dealing with complex risks in systems characterized by feedback loops, tipping points and opaque cause-and-effect relationships that can make intervention problematic.[51]

 © 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner®

Cybersecurity Isn't Just About Protecting Information Anymore

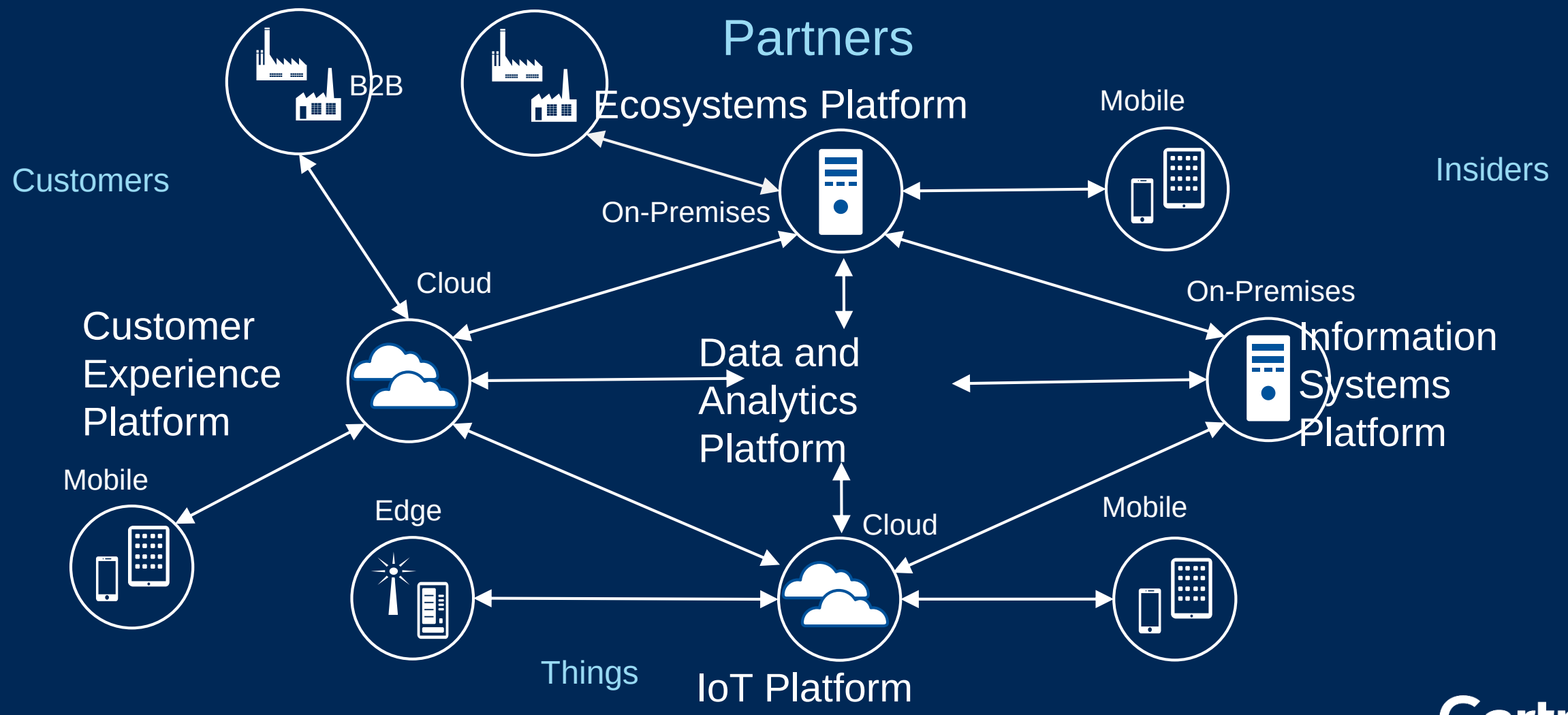


INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

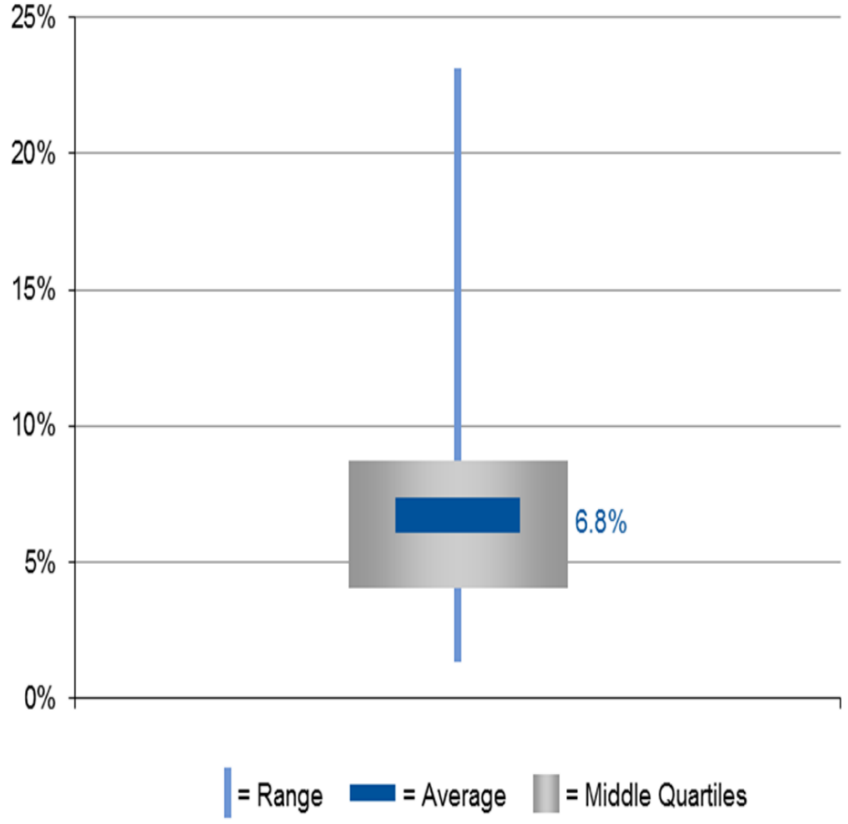
All Your Stuff Is Not Under One Roof



© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Not enough people, and there won't be for a while..



Total IT Security Support FTEs as a Percent of Total IT FTEs, 2018

Which of these technologies will require (has required) …

Impact of technologies on the IT department

Technology	Size of sample using this technology	Needed new skills	Needed hard-to-find skills	Needed change to structure of IT	Needed change to culture of IT	Needed new IT leadership	Needed new source of funding
Digital security	2,242	26%	22%	14%	18%	12%	11%
Internet of Things	1,115	25%	10%	21%	16%	14%	21%
Artificial intelligence	807	47%	37%	22%	29%	27%	21%
Conversational interfaces	654	5%	4%	5%	8%	3%	3%
3D printing	522	1%	0%	1%	0%	0%	3%
Smart robots	512	8%	6%	9%	10%	8%	9%
Virtual/ augmented reality	524	8%	6%	5%	4%	5%	9%
Digital twin	381	9%	6%	9%	12%	9%	7%
Blockchain/ distributed ledger	293	23%	18%	13%	14%	11%	17%
Autonomous vehicles	208	8%	10%	7%	5%	7%	15%

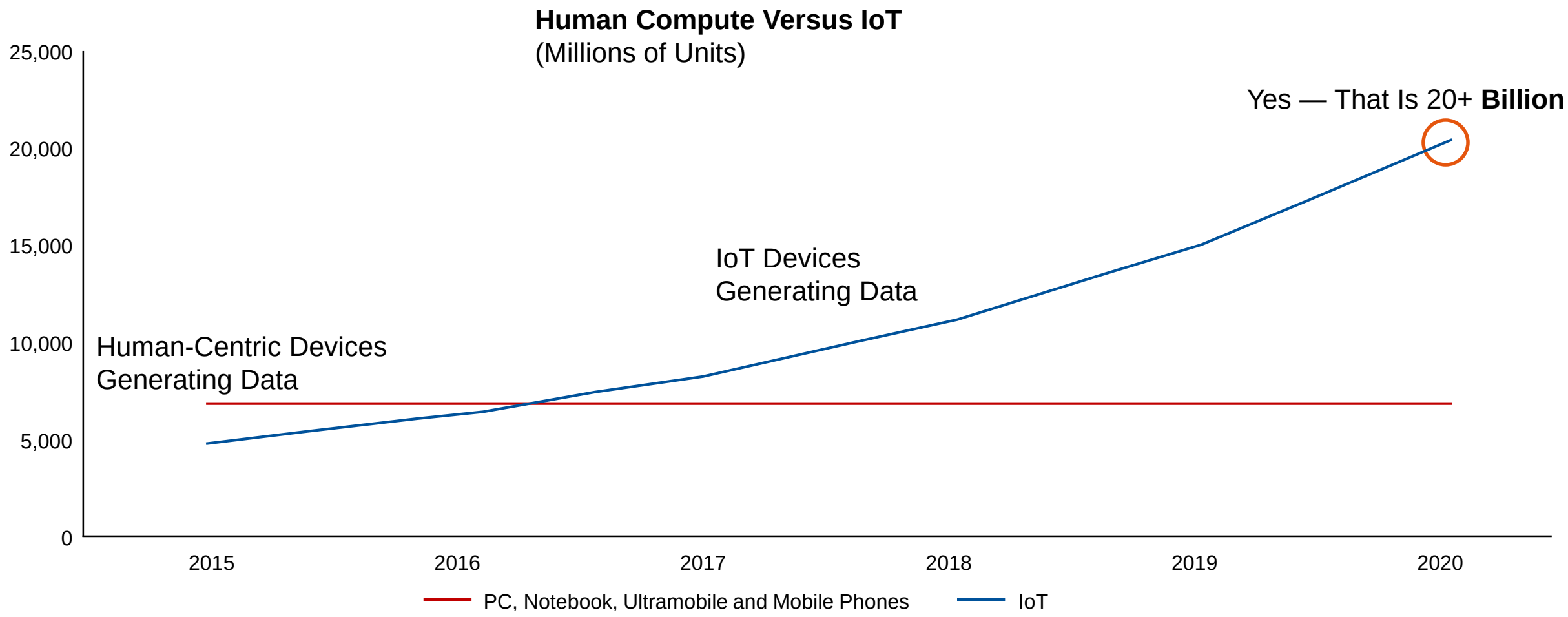
Colors show an impact "heat map," with grays denoting the biggest impact, blues the least.

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

You Have Many "Things" …



Source: Gartner 2016

INTERNAL or RESTRICTED

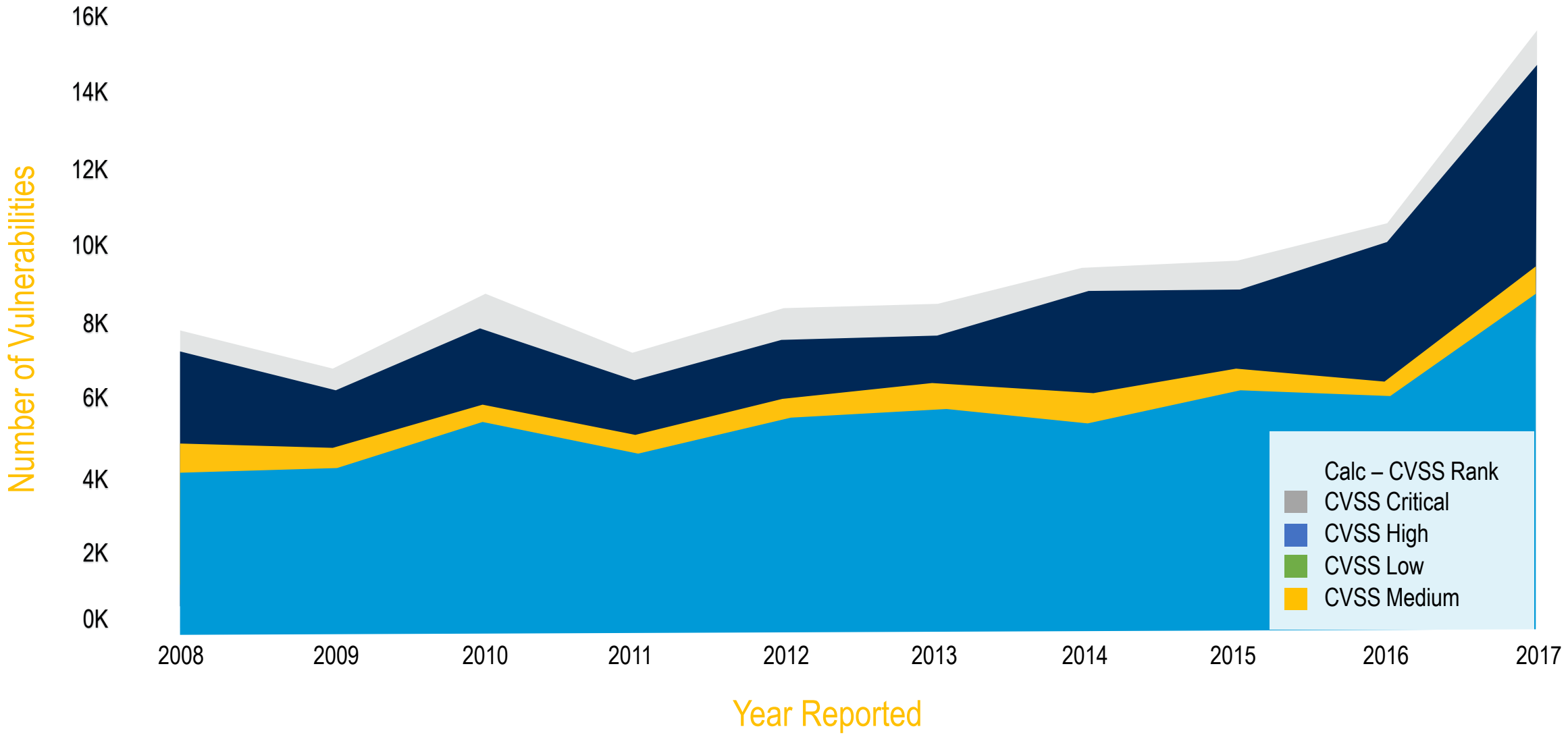
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

These passwords give access to over 500,000 IoT Devices TODAY

supervisor, supervisor
admin, meinsm
root, xmhdipc
admin1, password
root, admin
root, dreambox
888888, 888888
root, 00000000
admin, 1111111
root, pass
admin, 1234
administrator, 1234
root, 12345
tech, tech
admin, 1111
guest, guest
root, anko
root, default
admin, admin
666666, 666666
root, klv1234
service, service
admin, *(none)*
root, 54321
admin, password
admin, admin1234
admin, 54321
admin, smcadmin
root, user
root, 1111
root, jvbzd
root, 7ujMko0admin
root, system
admin, 12345
admin, 123456
Administrator, admin
user, user
root, zlxx
root, *(none)*
root, Zte521
support, support
root, 123456
guest, 12345
root, 888888
root, xc3511
root, password
root, klv123
root, hi3518
admin, pass
admin, 7ujMko0admin
root, vizxv
root, 666666
root, juantech
ubnt, ubnt
root, 7ujMko0vizxv
root, 1234
root, ikwb
root, realtek
root, root

Can you imagine the implications of 20B+ Devices?

Your Roofs Are Leaky, and Getting Leakier



INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

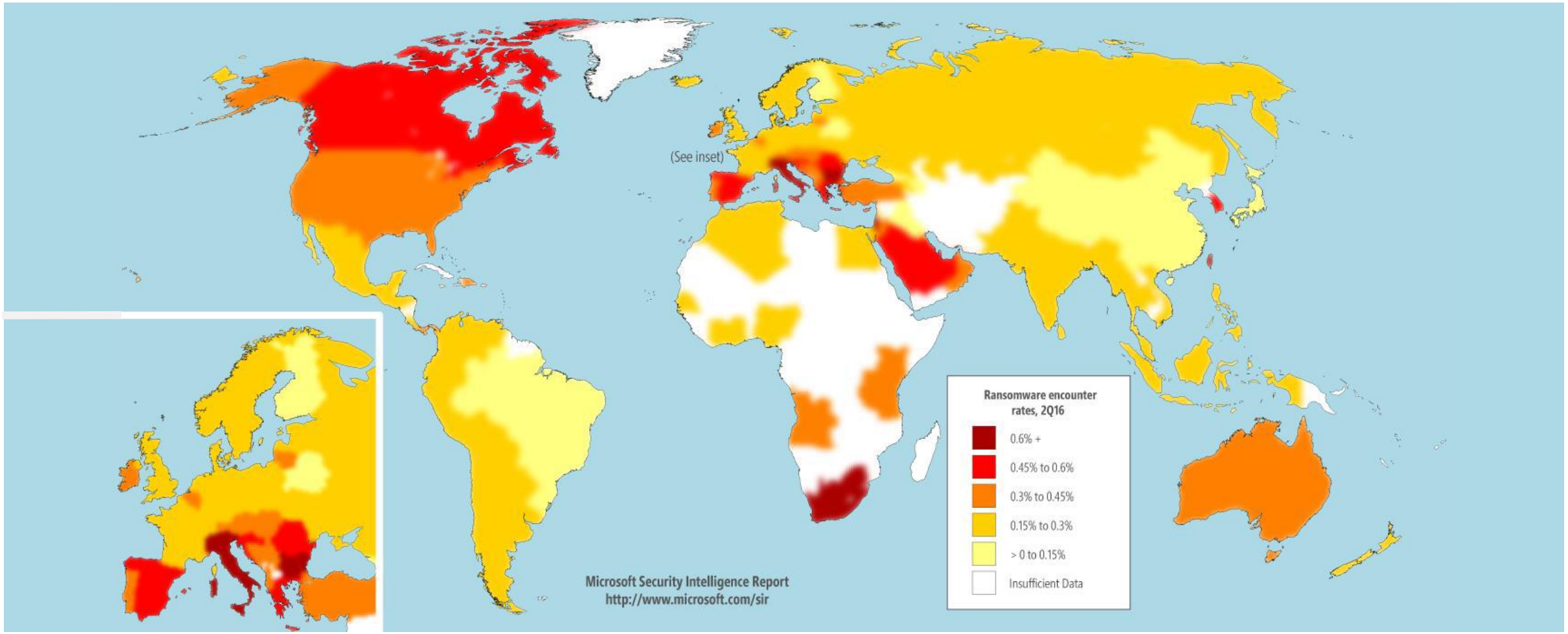
The Monetization of Threats — Ransomware

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

The Ransomware Weather Map



Source: Microsoft: Ransomware by Region 2Q17

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

The Monetization of Threats — Cryptomining Malware

Show 10 entries

Search:

Model	Hashrate	Algorithm	Power (watts)	Core clock	Memory clock	Manufacturer	Base	MoreInfo
Radeon Rx 480	25 MHash/s	Ethereum	150	1120 MHz	-	Sapphire	AMD	More →
Radeon Rx 470	24 MHash/s	Scrypt	150	1143	-	Sapphire	AMD	More →
Radeon R9 280X	18 MHash/s	Scrypt	180	900 MHz	-	Sapphire	AMD	More →
Radeon R9 290x	23.2 MHash/s	Ethereum	-	-	-	Sapphire	AMD	More →
GTX 760	6.4 MHash/s	Ethereum	170	980	-	Gigabyte	Nvidia	More →
Radeon R9 280x	22.4 MHash/s	Ethereum	180	900 MHz	-	Sapphire	AMD	More →
GeForce GT 750M	0.45 MHash/s	Ethereum	55	1033	-	Gygabyte	Nvidia	More →
HD 7870	12.2 MHash/s	Ethereum	-	1100 MHz	-	Gigabyte	AMD	More →
GeForce 840M	1.66 MHash/s	Ethereum	-	-	-	Nvidia	Nvidia	More →
GeForce GTX 560M	1.85 MHash/s	Ethereum	-	1550 MHz	-	Nvidia	Nvidia	More →

Showing 1 to 10 of 131 entries

Previous 1 2 3 4 5 … 14 Next

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

State-Sponsored Malware is becoming more sophisticated

We started with Stuxnet targeting Iran

Shamoon and StoneDrill wipers. Targeting Saudi infrastructure

Project Sauron. Targets air-gapped machines and defeats USB-blocking DLP. 50+ modules.

Flame/SkyWiper. Records audio, keyboard, Skype, net traffic.
Middle East links.

List of code names for various families of modules in Flame's source code and their possible purpose

Name	Description
Flame	Modules that perform attack functions
Boost	Information gathering modules
Flask	A type of attack module
Jimmy	A type of attack module
Munch	Installation and propagation modules
Snack	Local propagation modules
Spotter	Scanning modules
Transport	Replication modules
Euphoria	File leaking modules
Headache	Attack parameters or properties

INTERNAL or RESTRICTED

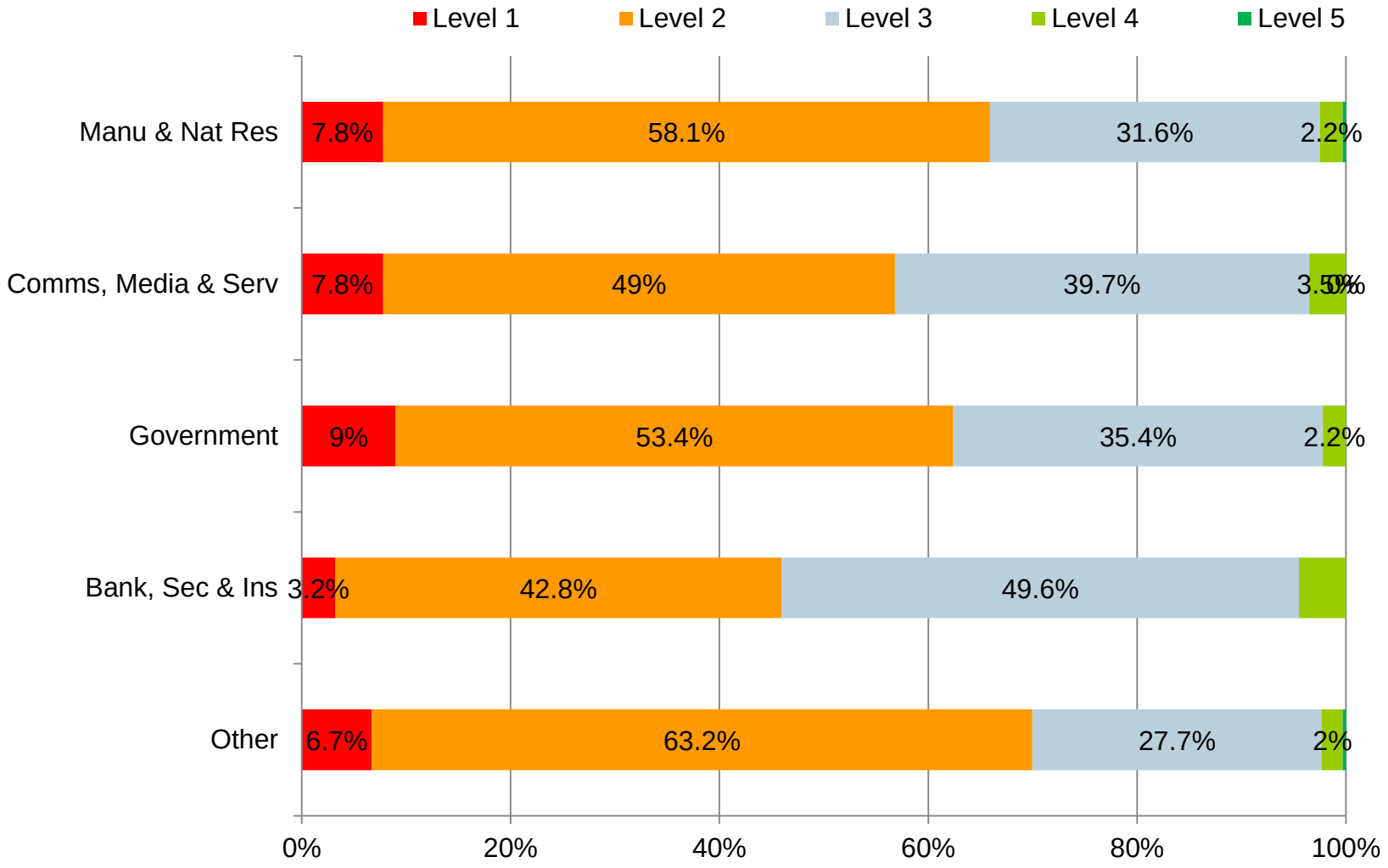
© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

The Perfect Storm: How Many Zero Days?

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

What about Maturity?

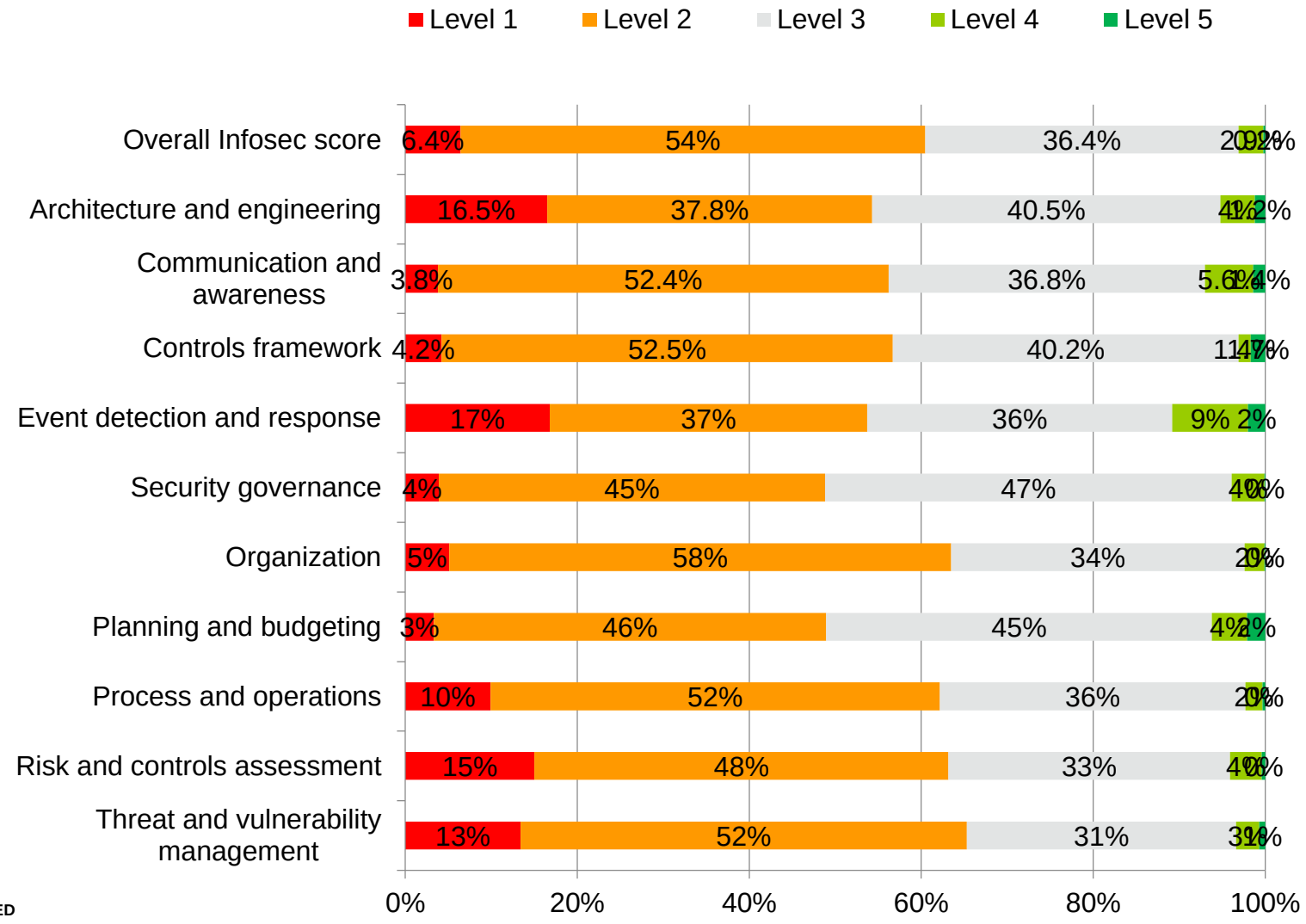
N = 2890 end users



INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Discipline score distribution



INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Stop Counting Threats

Stop Scaring Scared People

Use Your Humans Wisely

Patch Your Things, Do Your Best

Watch the Weather: Keep Detecting

Plan for Future Trends Now

Fix That Leaky Roof

And Carry an Umbrella

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner®

Top Trends

Ongoing strategic shifts in the security ecosystem that are expected to have significant potential for disruption

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

1

“Senior Executives Are Finally Aware That Cybersecurity Has a Significant Impact on the Ability to Achieve Their Goals …”

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Security Failures Are Impacting Business Goals

Verizon received a $350M discount on their purchase of Yahoo! as a result of Yahoo's data breach, which resulted in a failure to hit the standard of due care

Equifax's breach cost the CEO, CIO and the CSO their jobs and will have continuing significant financial impact

Maersk took a $300M expense as a result of a massive ransomware attack

Global economic losses from "WannaCry" attack was estimated to be between $1.5 billion and $4 billion

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

In Order to Capitalize on This Trend, Leading Security Organizations Are …

- Understanding business risk appetite and risk tolerance
- Articulate all risks within the context of business objectives
- Developing better board and security partnerships
- Establishing service levels that align with business risk
- Improving their digital business resilience

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

2

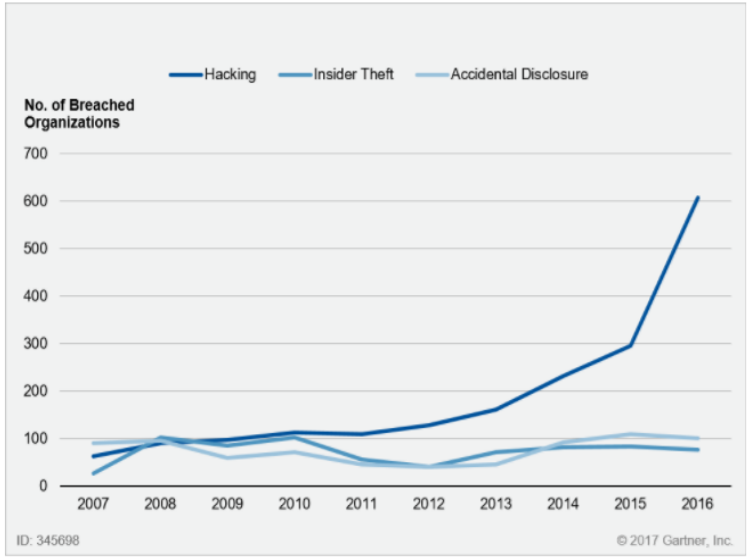
“Legal and Regulatory Mandates on Data Protection Practices Are Impacting Digital Business Plans and Demanding Increased Emphasis on Data Liabilities.”

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Data Liabilities Increase

Figure 1. Number of Organizations in the U.S. That Suffered a Data Breach



Source: Gartner (November 2017)

Based on data points sourced from "2017 Data Breaches" from the Identity Theft Resource Center.

Brand damage

Compliance

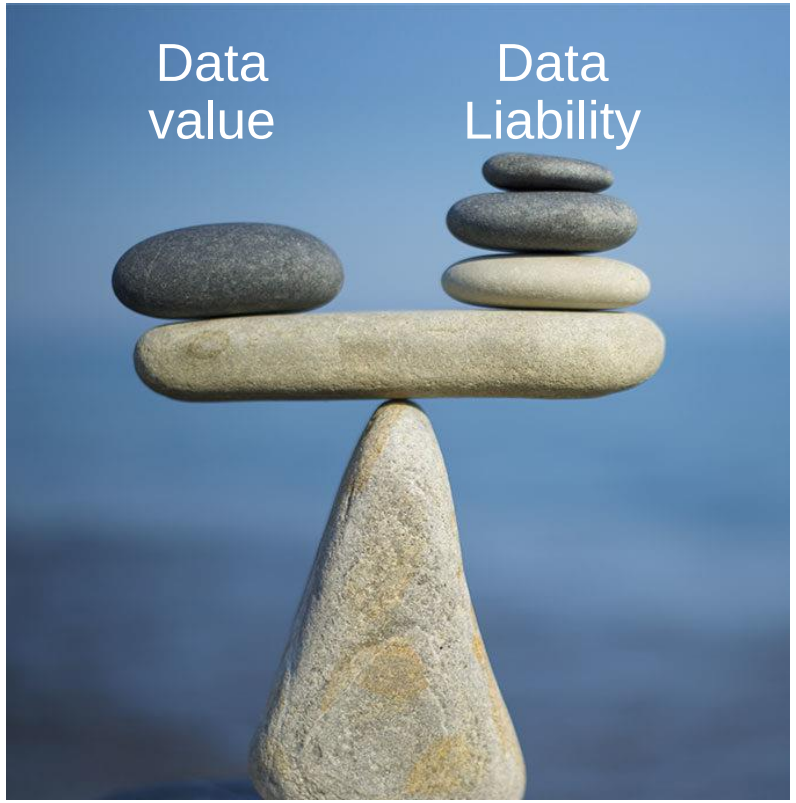
Protection

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

Leading Security Organizations Are …

- Using the full liability costs of data in digital business plans.
- Eliminating or offloading data when liability exceeds value
  - Trusted third-party providers, anonymized data or establish policies to delete sensitive data that is no longer useful.
- Differentiating with transparency and trust



Digital business

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

3

“Security Products Are Rapidly Exploiting Cloud Delivery to Provide More Agile Solutions.”

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Why Cloud?

- Accuracy
- Agility
- Freshness
- Extensible
- Staff augmentation

Why Not Cloud?

- Data sensitivity?
- Concentration of risk

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Leading Security Organizations Are …

- Critically reviewing new on-premises security solutions
- Investing in more agile cloud and service delivery solutions with:
  - A data management and machine learning competency
  - Staff augmentation services
  - API-enabled services

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

4

“Machine Learning Is Providing Value in Simple Tasks and Elevating Suspicious Events for Human Analysis.”

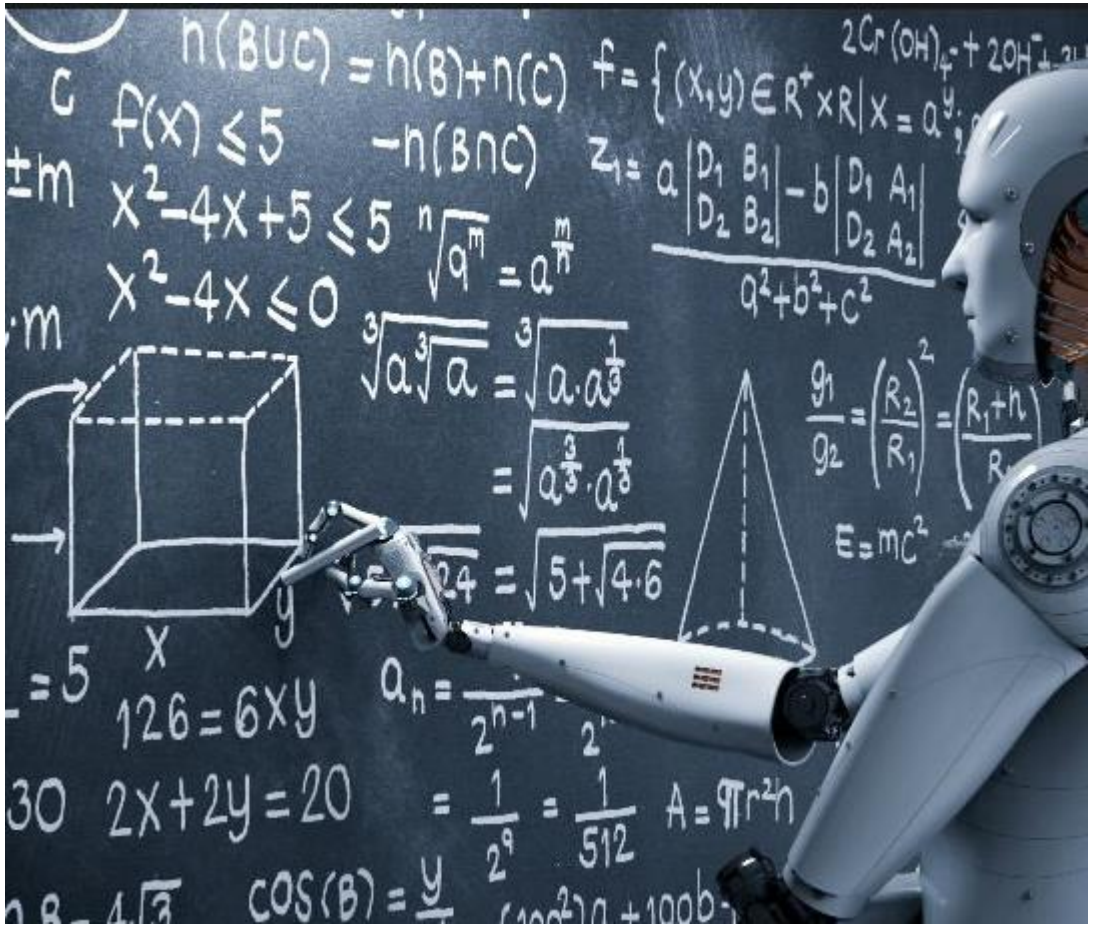
INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

There Is Value

- More constrained problems
- Grouping files
- Fraud
- Adaptive authentication
- Insider threats

But …

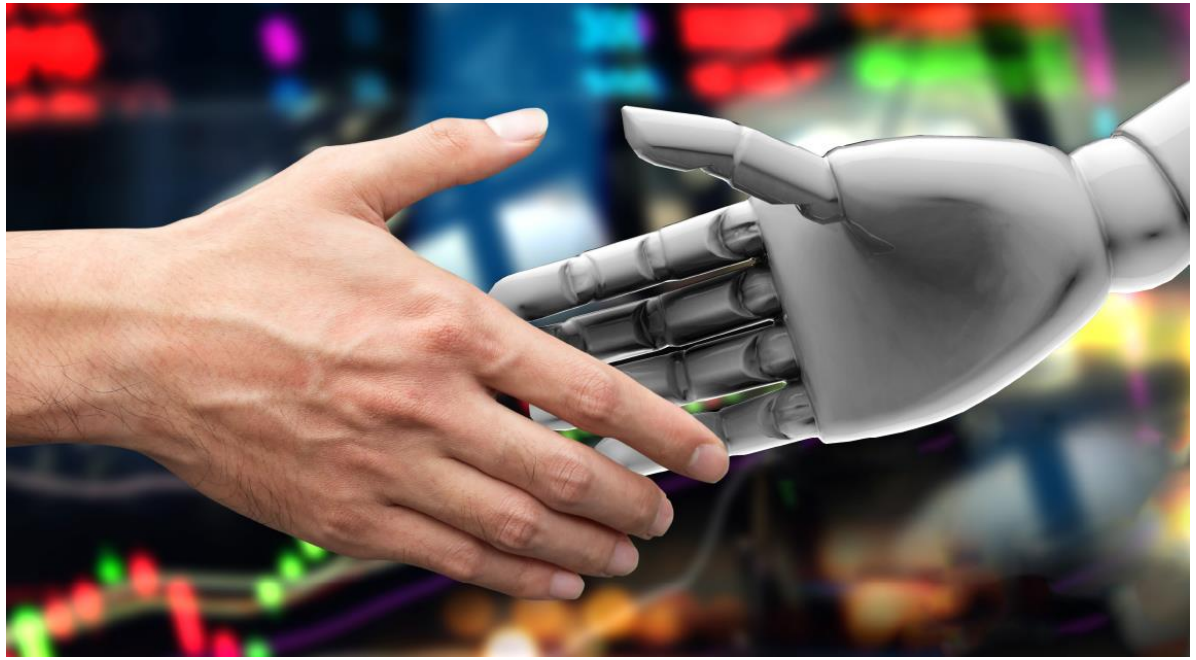


INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Nothing Is Perfect

We cannot escape the fact **that Humans and machines complement each other** and together can outperform either alone.

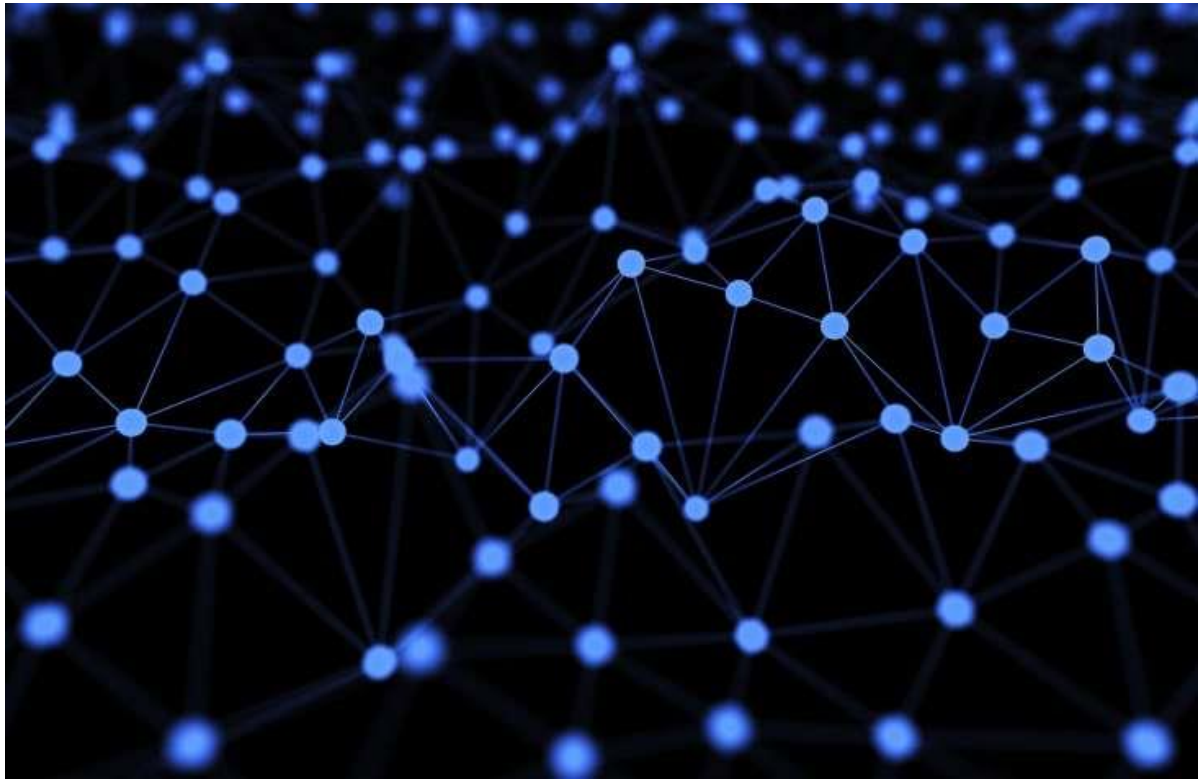


INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Leading Security Organizations Are …

- Implementing machine learning enhanced products to enhance or augment human resources
- Investing in skills to interpret and augment machine learning
- Demanding proof of vendor claims of machine learning based on measurable outcomes



INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

5

“Security Buying Decisions Are Increasingly Based on Geopolitical Factors Along With Traditional Buying Considerations.”

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

A Cold War Is Raging in Cyberspace

BEST DEFENSE

NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons

Not many people noticed it, but last month, NATO made a dramatic change in its cyber policy.

BY THOMAS E. RICKS | DECEMBER 7, 2017, 10:15 AM

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Leading Security Organizations Are …

- Taking geopolitical risk into consideration in purchasing decisions
- Sensitive to the geopolitical security demands of business relationships
- Aware that security and product buying decisions are based in **trust** in the integrity of the supplier

INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

You should really care now…

Top 10 Business Priorities	All Government (n = 379)	Local Government (n = 103)	State or Province (n = 90)	National or Federal (n = 143)	Defense and Intelligence (n = 35)	All Others (n = 2,236)
Digital business/digital transformation	18%	15%	20%	24%	6%	17%
Security, safety and risk	13%	18%	16%	6%	23%	
Governance, compliance, regulations	12%	13%	8%	14%	11%	
Technology initiatives/improvements	11%	12%	12%	10%	11%	6%
Service improvements/optimization	9%	13%	11%		14%	
Innovation, R&D, new products/services	9%	12%	8%	8%	6%	10%
Analytics/data/information	8%			11%		
Process improvement/optimization/automation	7%		13%	8%	9%	
Productivity/optimization/efficiency	7%	9%	7%		6%	
Sustainability/social responsibility	7%	13%		6%		
Infrastructure development/transformation		10%				
Growth/market share		9%				30%
Financial health			7%			
Customer focus			6%	8%		9%
Operations improvement/efficiency/excellence				8%	14%	6%
Workforce focus					11%	
Profit improvement/profitability/asset monetization						12%
Corporate/M&A/new business/consolidation						8%
New customers/retention/sales						7%
Cost optimization/management/reduction						7%

Percentage of Respondents

Base: All answering; 10 top ranked items per segment, excluding "don't know" responses; n varies by segment.
Q. Thinking about your organization as a whole, what would you say are its top business objectives for the next two years (2017/2018)?

© 2017 Gartner, Inc.

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Gartner

Gartner can help!

- Top Security and Risk Management Trends
- Cybersecurity and Digital Risk Management: CIOs Must Engage and Prepare
- Modern Privacy Regulations Could Sever or Strengthen Your Ties With Customers
- How to Evaluate Cloud Service Provider Security
- Artificial Intelligence and Application Security Vendors: Marketing Hype or Genuine Hope?

For information, please contact your Gartner representative.
INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.

Toolkits!

- Best Practices for Creating an Enterprise Information Security Charter (with templates)
- Simple Functional Information Security Taxonomy
- Research Roundup for Creating Information Security Policy
- Best Practices for Establishing an Information Security Steering Committee
- Security Management Strategy Planning Best Practices
- ITScore for Information Security
- Creating a Security Process Catalog
- Information Security Organization Dynamics

For information, please contact your Gartner representative.
INTERNAL or RESTRICTED

© 2018 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates.