Welcome to Auto-ISAC!

Monthly Virtual Community Call

December 2, 2020

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ What's Trending
11:15	***DHS CISA Community Update***
11:20	**Featured Speaker: Dr. Larry Ponemon**: *Chairman and Founder of the Ponemon Institute*, **Rocco Grillo**: *Managing Director at Alvarez & Marsal*, **Charlie Miller**: *Senior advisor at The Santa Fe Group*
11:45	**Around the Room** ➢ Sharing Around the Virtual Room
11:55	**Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:

- ✓ *Stay informed of Auto-ISAC activities*
- ✓ *Share information on key vehicle cybersecurity topics*
- ✓ *Learn about exciting initiatives within the automotive community from our featured speakers*

Participants: Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government – *the whole of the automotive industry*

Classification Level: **TLP:GREEN -** May be shared within the Auto-ISAC Community and "off the record"

How to Connect: For further info, questions or to add other POCs to the invite, please contact us! (lisascheffenacker@automotiveisac.com)

Engaging in the Auto-ISAC Community

19 *Navigator Partners*

❖ Join

- ❖ If your organization is eligible, apply for Auto-ISAC membership
- ❖ If you aren't eligible for membership, connect with us as a Partner
- ❖ Get engaged – *"Cybersecurity is everyone's responsibility!"*

❖ Participate

20 *OEM Members*

- ❖ Participate in monthly virtual conference calls (1st Wednesday of month)
- ❖ If you have a topic of interest, let us know!
- ❖ Engage & ask questions!

12 *Innovator Partners*

❖ Share – *"If you see something, say something!"*

36 *Supplier & Commercial Vehicle Members*

- ❖ Submit threat intelligence or other relevant information
- ❖ Send us information on potential vulnerabilities
- ❖ Contribute incident reports and lessons learned
- ❖ Provide best practices around mitigation techniques

Membership represents **99%** *of cars on the road in North America*

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

2020 Board of Directors

Executive Committee (ExCom)

Kevin Tierney
Chair of the Board of the Directors
GM

Josh Davis
Vice Chair of the Board of the Directors
Toyota

Jenny Gilger
Secretary of the Board of the Directors
Honda

Tim Geiger
Treasurer of the Board of the Directors
Ford

Todd Lawless
Chair of the Advisory Board
Continental

2020 Advisory Board (AB) Leadership

Todd Lawless
Chair of the Advisory Board
Continental

Brian Murray
Vice Chair of the Advisory Board
ZF

Chris Lupini
Chair of the SAG
Aptiv

Larry Hilkene
Chair of the CAG
Cummins

Member Roster

As of December 2, 2020

Highlighted = Change

Aisin	Honda	PACCAR
Allison Transmission	Hyundai	Panasonic
Aptiv	Infineon	Qualcomm
Argo AI	Intel	Renesas Electronics
AT&T	Kia	Subaru
Blackberry Limited	Knorr Bremse	Sumitomo Electric
BMW Group	Lear	Tokai Rika
Bosch	LGE	Toyota
Continental	Magna	TuSimple
Cummins	MARELLI	Valeo
Delphi Technologies	Mazda	Veoneer
Denso	Mercedes-Benz	Volkswagen
FCA	Mitsubishi Motors	Volvo Cars
Ford	Mitsubishi Electric	Volvo Group
Garrett	Mobis	Waymo
General Motors	Navistar	Yamaha Motors
Geotab	Nexteer Automotive Corp	ZF
Google	Nissan	
Harman	NXP	
Hitachi	Oshkosh Corp	TOTAL: 57

Auto-ISAC Activities

- **Auto-ISAC Virtual Summit Oct 14-15 – Completed**

- **Other Key Auto-ISAC Member Events -**
  1. **Member Survey: COMPLETED**
  2. **ETSC Event:**
     a) **Tuesday, December, Aptiv presenting on: *"Risk Assessment Methodology for 21434 Compliance".***
     b) **Wednesday, December 9 presentation by T. Gaertner (BMW) *"Security Testing".***
  3. **All Member's Meeting: Wednesday, Dec 2nd 1-3 pm**
  4. **Advisory Board Meetings: Thursday, Dec 3rd, 9-12 pm**
  5. **Board of Directors Meeting: Thursday, Dec 3rd, 2-4 pm**

Security architectures are only as strong as their implementation in the final product.

This Bluetooth Attack Can Steal a Tesla Model X in Minutes

Lennert Wouters, a security researcher at Belgian university KU Leuven, today revealed a collection of security vulnerabilities he found in both Tesla Model X cars and their keyless entry fobs.

Wouters states the following regarding Tesla's security issues: "[Tesla's] system has everything it needs to be secure … there are a few small mistakes that allow me to circumvent all of the security measures." Though many cybersecurity teams spend significant amounts of time on security architectures, it is the responsibility of developers and other engineers to properly implement controls.

This One Time on a Pen Test: How I Hacked a Self-Driving Car

An organization hired us to perform a penetration test on a self-driving car—as it turns out, there are several self-driving projects available on the market today, so we were tasked with assessing the attack surface of the vehicle to enumerate vulnerabilities that could lead to remote control of the vehicle.

This report points out valuable learnings from a pentest on an undisclosed autonomous driving platform. While this report is not very technical, there are a few key takeaways:

- *Sufficiently harden or disable exposed services (e.g., FTP).*
- *Apply known best practices for Docker containers.*

Further Reading: https://www.telematicswire.net/magazine/2020/nov/

For more information or questions please contact analyst@automotiveisac.com

CISA RESOURCE HIGHLIGHTS

TLP:WHITE - ICT SCRM Task Force: Lessons Learned During the COVID-19 Pandemic Report

- **Developed by the Information and Communications Supply Chain Risk Management (ICT SCRM) Covid-19 Impact Study Working Group, released by DHS on November 5, 2020**
- **Examines how the COVID-19 pandemic impacted the logistical supply chains of information and communication technology (ICT) companies**
- **Provides recommendations on how organizations can increase their supply chain resilience from future risks**
- **Available for download at:**
  - **https://www[.]cisa[.]gov/sites/default/files/publications/lessons-learned-during-covid-19-pandemic_508_1.pdf**

Chemical Security Summit 2020

- **Hosted by CISA and the Chemical Sector Coordinating Council (SCC)**
- **Signature industry event for chemical representatives across the chemical and interconnected sectors**
- **Virtual seminars take place on December 2, 9, and 16**
- **Register for the event at https://web[.]cvent[.]com/event/7c78ebd7-451e-445d-ae44-eb0b1ea3e7e7/summary**
- **Agenda is available for review at https://www[.]cisa[.]gov/publication/2020-chemical-security-seminars-agenda**

TLP: WHITE – Current Activity – Online Holiday Shopping Scams

- **CISA is providing this reminder and resources to encourage vigilance in the midst of increased online commerce during the 2020 holiday season**
- **The Current Activity provides links to CISA's Online Shopping Tips, FBI resources, and guidance on how to report incidents**
- **See https://us-cert[.]cisa[.]gov/ncas/current-activity/2020/11/24/online-holiday-shopping-scams for more details**

TLP: WHITE – CISA Current Activity – Fortinet FortiOS System File Leak

- **CISA is aware of the possible exposure of passwords on Fortinet devices that are vulnerable to CVE 2018-13379**
- **Exploitation of this vulnerability may allow an unauthenticated attacker to access FortiOS system files**
- **Fortinet has released a security advisory that highlights mitigation of the noted vulnerability**
- **In addition to review and any necessary actions associated with the advisory, CISA recommends a careful review of logs on any connected networks to detect any additional threat actor activity**
- **Resources available at:**
  - **https://us-cert.cisa.gov/ncas/current-activity/2020/11/27/fortinet-fortios-system-file-leak**
  - **https://www.fortiguard.com/psirt/FG-IR-18-384**

TLP: WHITE – CISA Activity Alert AA20-336A - Advanced Persistent Threat Actors Targeting U.S. Think Tanks

- **Joint effort between CISA and the FBI**
- **Observed persistent intrusions by advanced persistent threat (APT) actors often targeting individuals and organizations that focus on international affairs or national security policy**
- **Resources used by the APT actors include spearphishing emails and third-party message services directed at both corporate and personal accounts. Exploitation of vulnerable web-facing devices and remote connection capabilities are also used**
- **Technical details, including ATT@CK framework resources are available at https://us-cert[.]cisa[.]gov/ncas/alerts/aa20-336a**

TLP: WHITE – Additional Resources From CISA

- CISA Homepage - https://www[.]cisa[.]gov/
- CISA News Room - https://www[.]cisa[.]gov/cisa/newsroom
- CISA Blog - https://www[.]cisa.gov/blog-list
- CISA Publications Library - https://www[.]cisa[.]gov/publications-library
- CISA Cyber Resource Hub - https://www[.]cisa[.]gov/cyber-resource-hub
- CISA Vulnerability Management (formerly known as the National Cyber Assessment and Technical Services (NCATS) program) - https://www[.]us-cert[.]gov/resources/ncats/
- CISA Cybersecurity Directives - https://cyber[.]dhs[.]gov/directives/
- CISA COVID-19 Response – https://www[.]cisa[.]gov/coronavirus

For more information:
cisa.gov

Questions?
CISAServiceDesk@cisa.dhs.gov
1-888-282-0870


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

30+ ***Featured Speakers to date***

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC

7 ***Best Practice Guides available on website***

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

2000+ ***Community Participants***

Slides available on our website – www.automotiveisac.com

Featured Speaker

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Dr. Larry Ponemon, Ponemon Institute

Chairman and Founder

Dr. Larry Ponemon is the Chairman and Founder of the Ponemon Institute, a research “think tank” dedicated to advancing privacy, data protection and information security practices. Dr. Ponemon is considered a pioneer in privacy auditing and the Responsible Information Management (RIM) framework. Security Magazine named him one of the “Most Influential People for Security.”

Ponemon consults with leading multinational organizations on global privacy management programs. He has extensive knowledge of regulatory frameworks for managing privacy and data security, including financial services, health care, pharmaceutical, telecom and Internet.

Rocco Grillo, Alvarez & Marsal

Managing Director, Global Cyber Risk Services

Rocco Grillo is a Managing Director at Alvarez & Marsal and leads the firm's Global Cyber Risk & Incident Response Investigations practice. He has over 20 years of experience providing clients cybersecurity advisory services, incident response investigations, and other technical advisory services, including providing guidance to C-suite and board members

Rocco has partnered with multiple government agencies, including the FBI, USSS, and the FTC in investigating and resolving a variety of cybersecurity and privacy breaches and has assisted clients with responding to some of the largest cyber-attacks and data breaches over the last 12 years. He has served as an affiliate board advisor to industry ISACs and has supported the development of the Financial Services-ISAC annual simulated Cyber-attack Against Payment Systems (CAPS) Exercise for over 8 years as well as the Retail & Hospitality-ISAC where we assisted them in conducting their first ever industry wide exercise last year.

Charlie Miller, The Santa Fe Group

Senior Advisor

Charlie Miller is a senior advisor at The Santa Fe Group where he is responsible for expanding the Shared Assessments Third Party Risk Management membership driven program, facilitating thought leadership, industry vertical strategy groups, continuous monitoring / operational technology working groups and IoT research studies.

Charlie has vast industry experience, having set up and led third party risk management and financial services initiatives for several global companies including AIG, BTMU, and Merrill Lynch.

Miller is a Distinguished Fellow of the Ponemon Institute, Certified International Privacy Professional and Certified Third Party Risk Professional.

SFG | SHARED ASSESSMENTS
The Trusted Source in Third Party Risk Management

AUTO-ISAC

Ponemon INSTITUTE

SHARED ASSESSMENTS – PONEMON INSTITUTE IOT RESEARCH

A New Roadmap for Third Party IoT Risk Management – The Critical Need To Elevate Accountability, Authority and Engagement

December 02, 2020

Rocco Grillo, Managing Director, Alvarez & Marsal
Charlie Miller, Senior Advisor, Shared Assessments
Larry Ponemon, Ph.D., Chairman and Founder, Ponemon Institute

Discussion Points

- Overview of Research Findings
- How Do Findings Relate to AUTO-ISAC Members
- IoT – You Know the Risks are Real!
- Recommendations & IoT To-Dos
- Resources & Contact Information

IoT → Internet of Everything

IoThings

- Information
- Consumer
- Operational

41.6 billion IoT Devices by 2025

80 ZB Data - 90% Unencrypted by 2025

57% of IoT devices are vulnerable to attacks

Challenges

- Innovation: Mobility ERA, Autonomous Vehicles
- Manufacturing: Automation / Plants / Supply Chain
- Information: ECU's, CAN's, OBD-II Dongel.s and Convivence Apps
- Integration: Auto Makers/Software Providers
- Transformation: US $1.3 Trillion Value by 2022
- Who's in the Drivers Seat?

Note: The survey for this Research Study was conducted in November 2019, prior to the Covid-19 Pandemic. As such, it does not include any risks related to IoT devices which are or may be used to support those individuals working from their homes. Therefore, no Consumer Technology IoT devices or applications were included in responses provided by survey respondents.

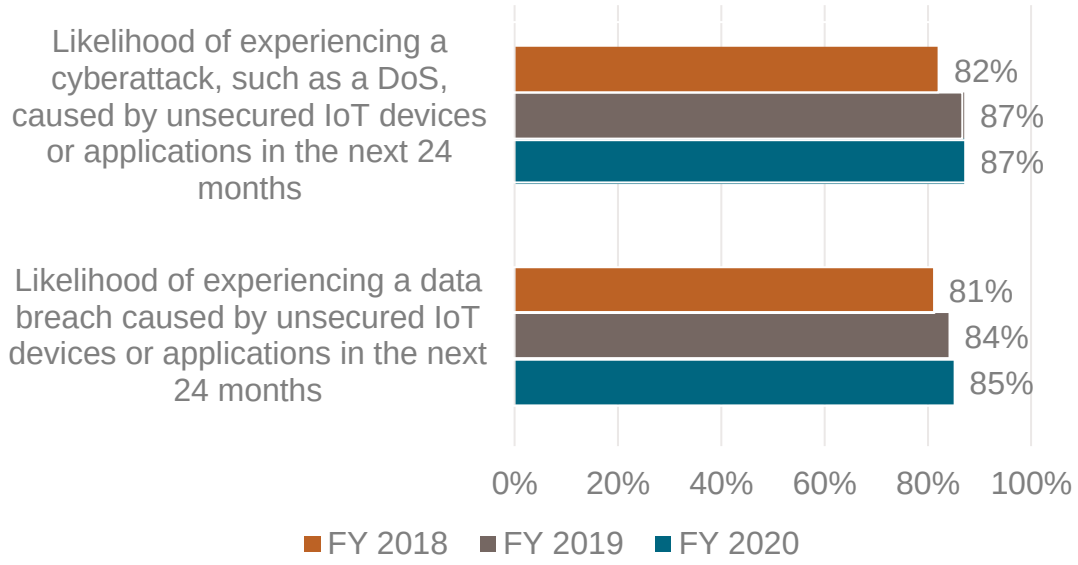
IoThreats

Year Over Year Trend Continues

- **Known data breaches caused by unsecure devices have doubled since 2017.**
- **Nearly nine out of 10 survey respondents expect their company to experience a cyber attack or data breach caused by unsecure IoT devices or applications in the next two years.**
- **More than three-quarters of respondents recognize that third party IoT risks pose a serious threat to their CROWN JEWELS.**

The likelihood <u>your organization</u> will have a data breach or cyber attack caused by unsecured IoT devices or applications in the next 24 months?

Very likely, Somewhat likely and Likely responses combined



Findings Overview

- **IoT use increasingly likely to have materially disruptive consequences.**
- **Business-related IoT devices will effectively double within next two years.**
- **Significant improvements are required in IoT hygiene practices in a vast majority of companies.**
- **Only 42% of companies can identify IoT devices with inadequate security.**
- **Actual breaches and cyberattacks caused by internal and third party IoT devices is significantly higher than reported.**
- **Few organizations are well-equipped to:**
  - manage IoT devices and applications; or
  - mitigate threats of data breaches, cyberattacks and IoT-associated threats

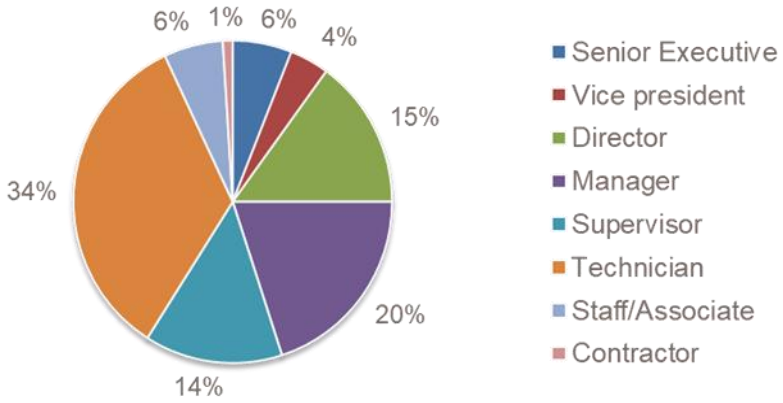
Source: A New Roadmap for Third Party IoT Risk Management – The Critical Need to Elevate Accountability, Authority and Engagement, 2020 Shared Assessments-Ponemon Research Report

This Year's Sampling Techniques

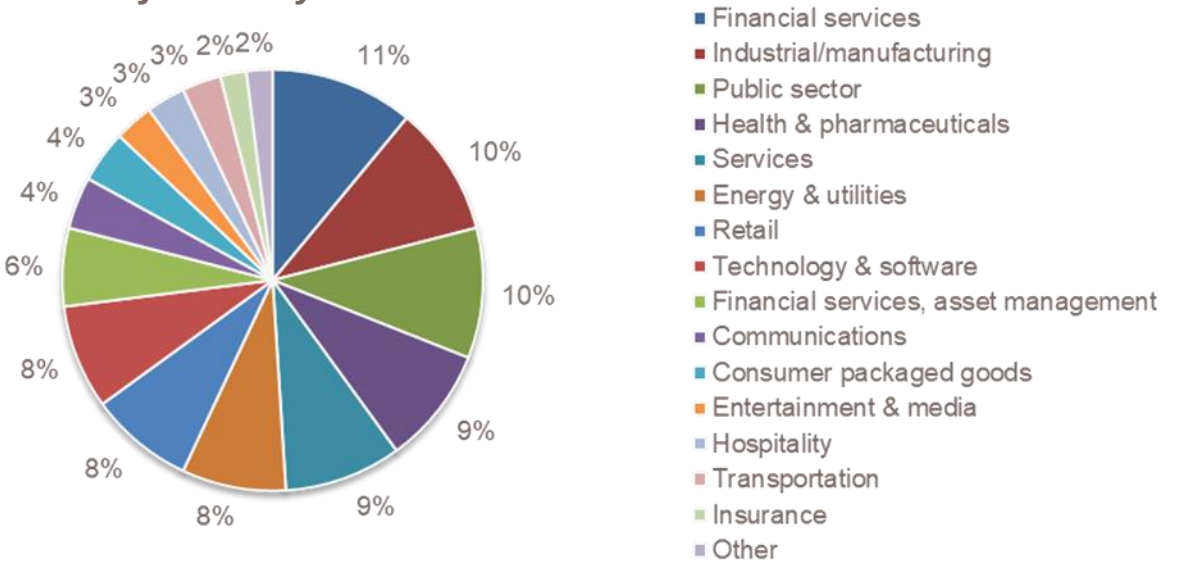
- **Additions**
  - **Sample size** – 630 individuals, familiar with the use of IoT devices in their organization and participate in corporate governance, third party risk management and/or risk oversight activities
  - **High Performers** – 164 respondents self-identified as "highly effective" – higher performers, 466 did not self-identify as higher performers
  - **Year-over-year comparisons** – 5% or greater are considered statistically significant

SURVEY RESPONSE	FY 2020	
Total sampling frame	16,902	
Total returns	713	
Rejected surveys	83	
Final Sample	630	**164** — Higher Performers
		466 — All Other Respondents
Response rate	3.7%	

Position



Primary industry

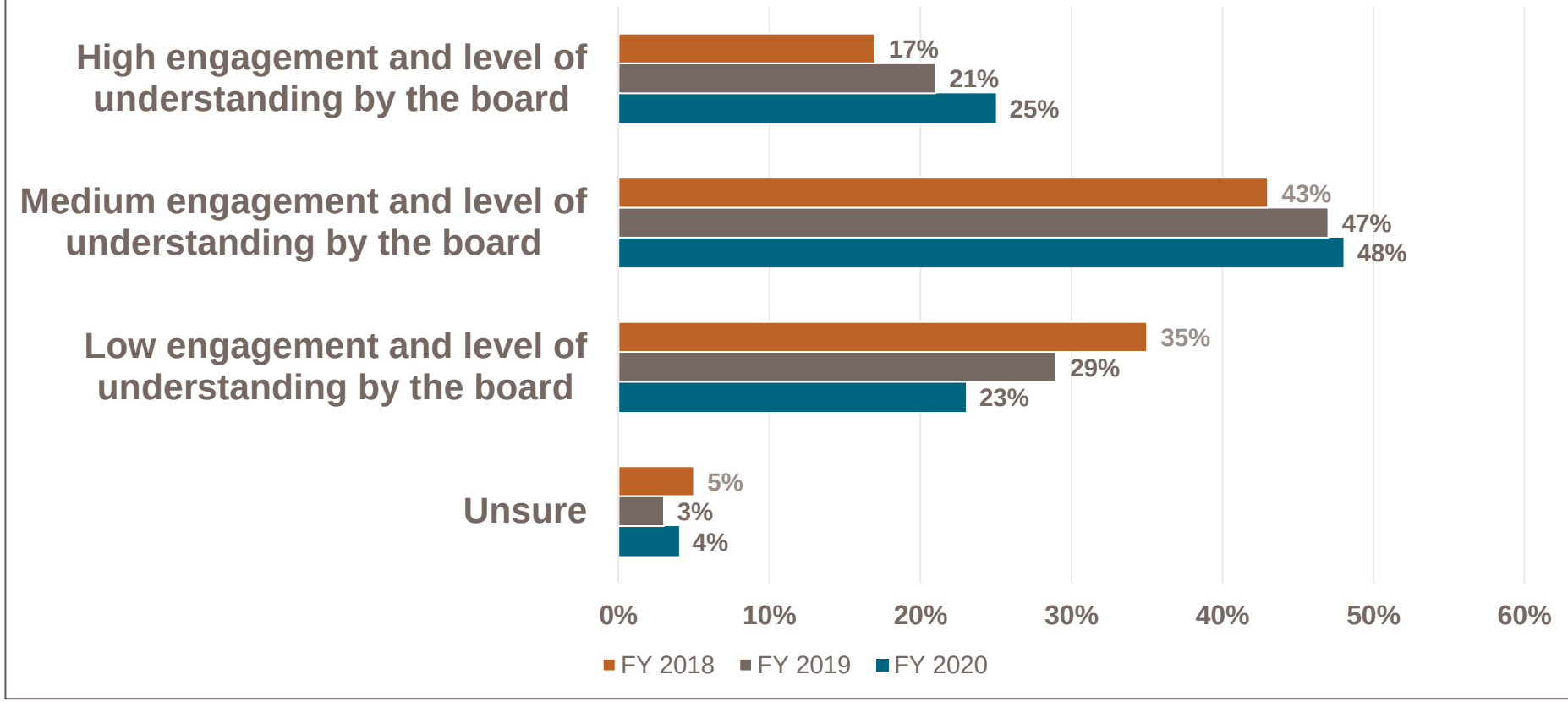


Leading Practices - Comparative

	Higher Performers	All Respondents	Key Practice Gaps
GOVERNANCE	73%	55%	• Low levels of board engagement with IoT risk • Lack of clearly defined IoT risk management accountability
Operate a TPRM Program approved by C-suite and/or board-level risk committee			
RISK MANAGEMENT	50%	31%	• Current IoT risk management programs not keeping pace with IoT risks • Represents and increasing strategic threat
Have incident response plans that include responses to incidents related to IoT			
ASSET MANAGEMENT	41%	25%	• Awareness of IoT risks remains relatively high • Awareness not translating into clear accountability to sufficiently drive improvements
Are aware of all or most of their IoT devices connected to the internet			
RESOURCE ALLOCATION	43%	35%	• Need for greater allocations for IoT risk management staff, budget, expertise and training
Report sufficient staff and budget are allocated to managing third party IoT risks			

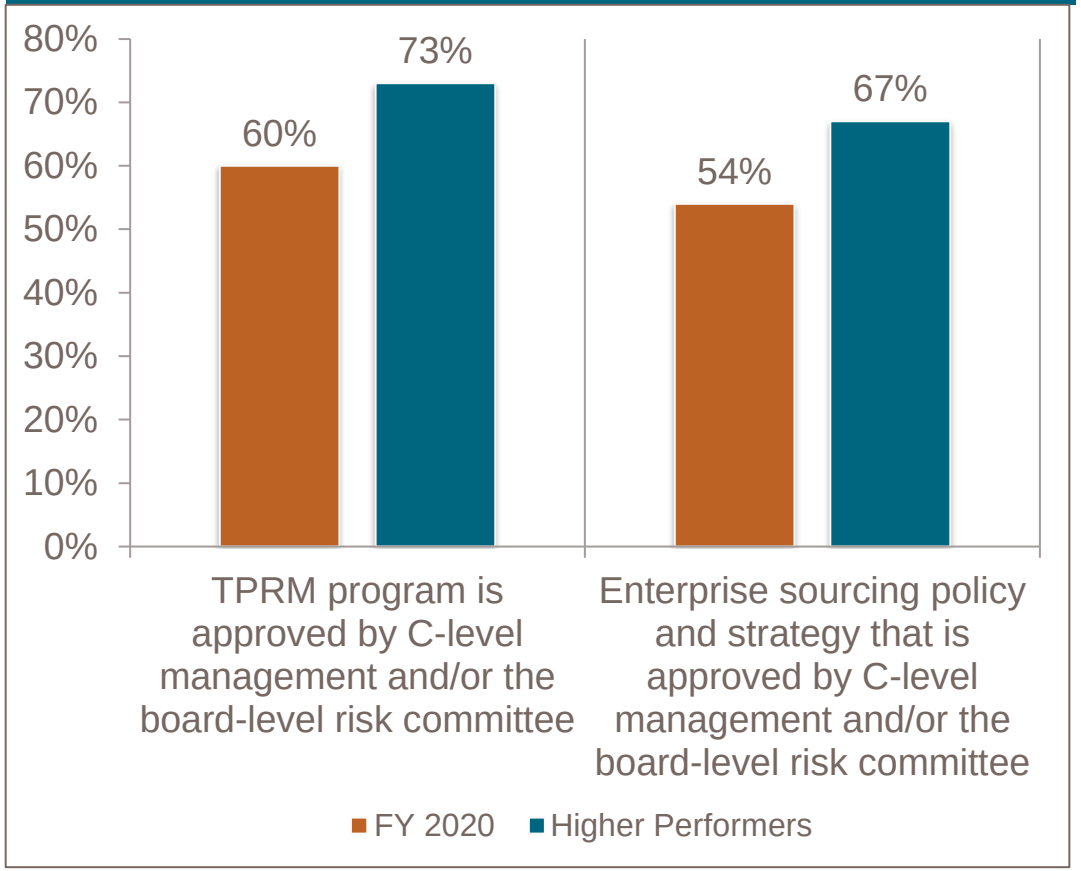
Board Governance

How engaged is your board of directors with third party cybersecurity risks?

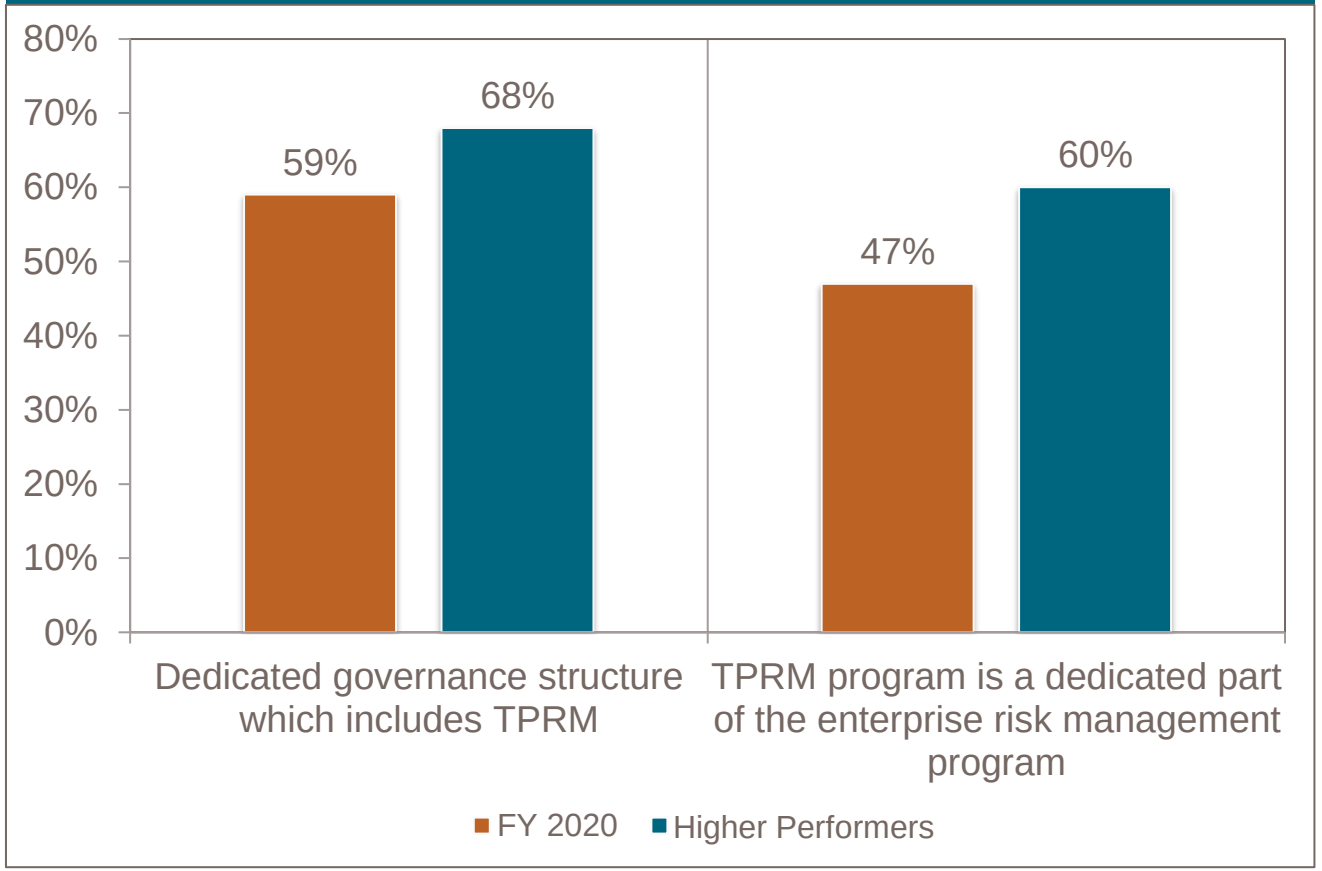


ERM Governance

C-level and board of directors involvement in managing Third Party risk



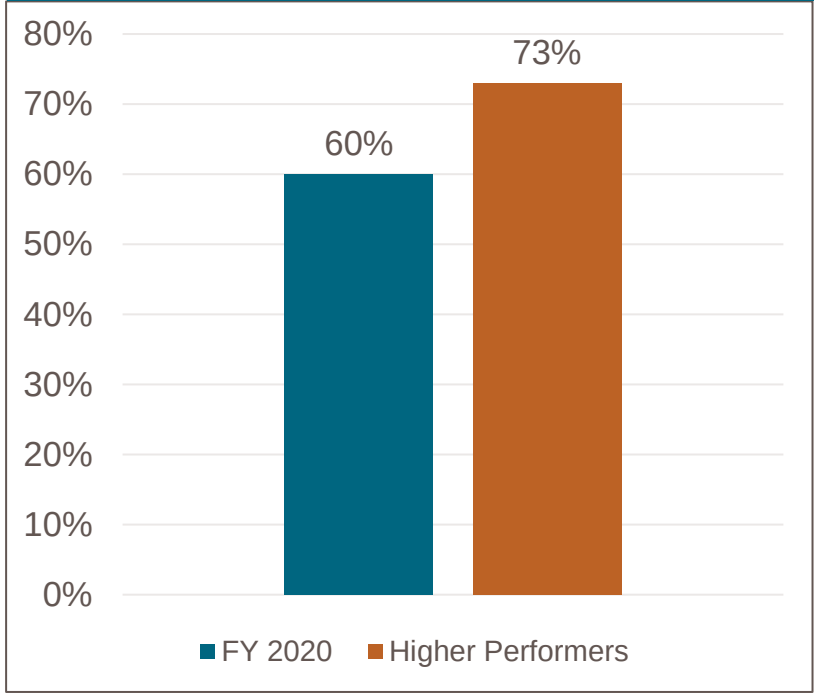
Organization includes TPRM in its governance structure and part of its enterprise risk management program?



Senior Level

C-level Governance & IoT Accountability

If your organization's TPRM program approved by C-level management or the board-level risk committee?



Yes responses shown

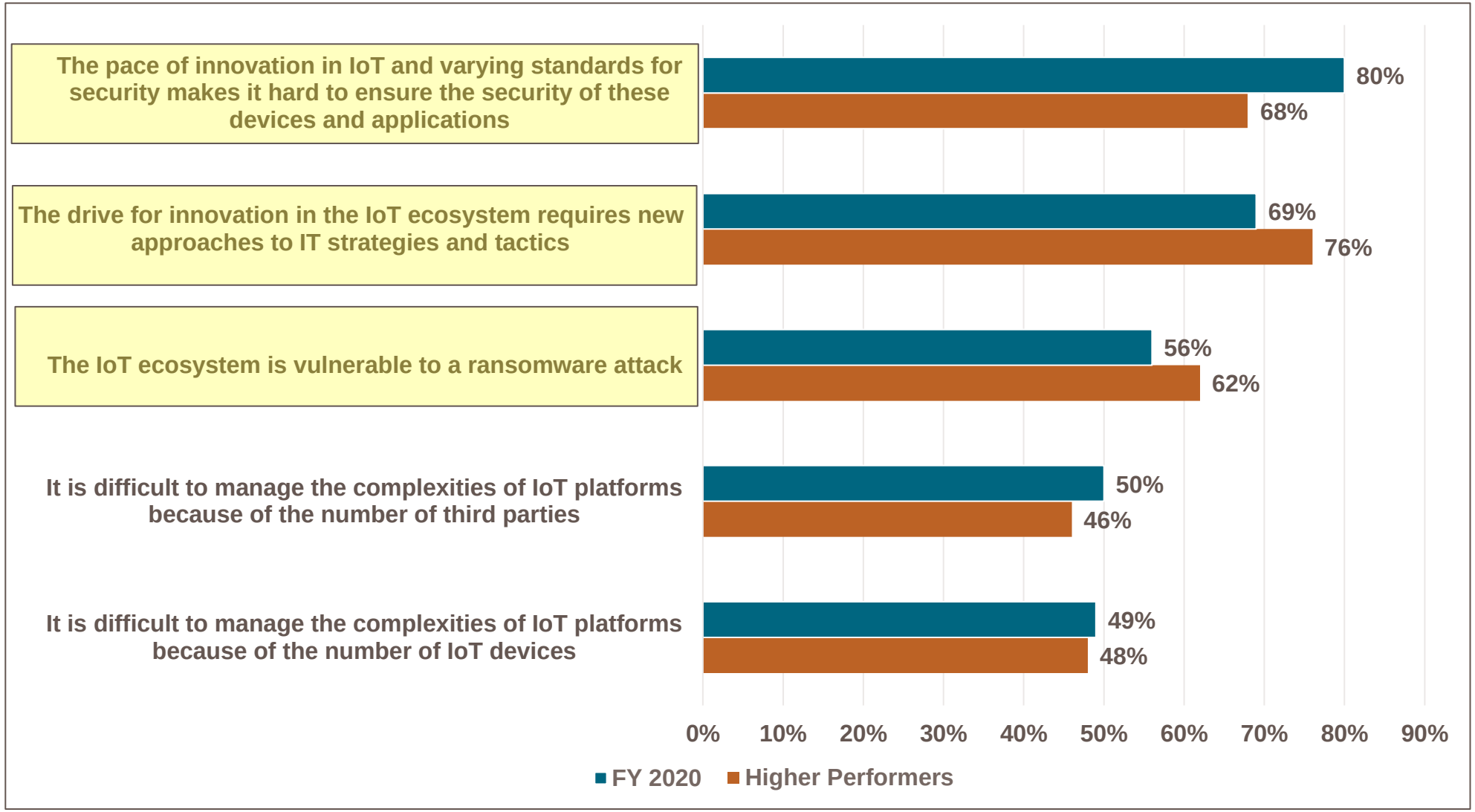
IoT Risk Is Increasing

Why?

Auto Industry

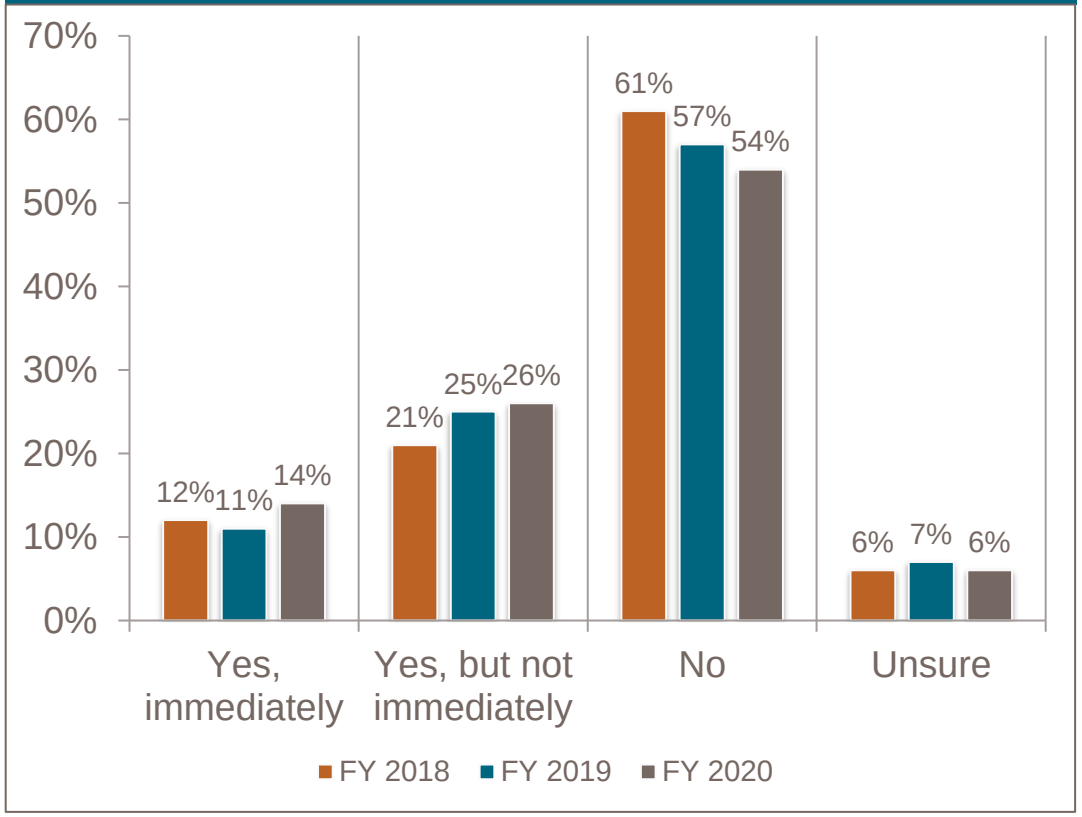
Connectivity and Convenience

A must have for consumers

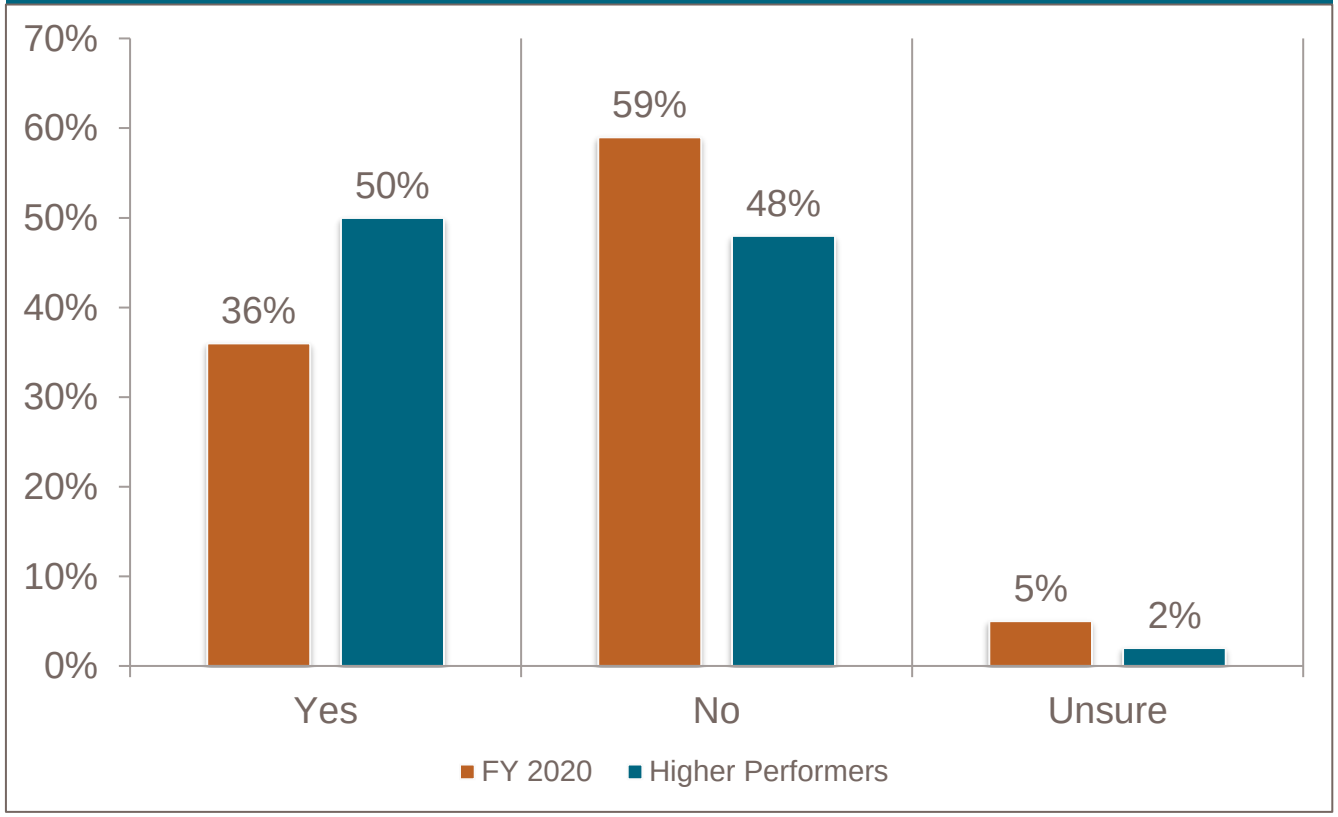


Risk Management

If your organization identifies unsecure IoT devices, do you replace them with secure devices

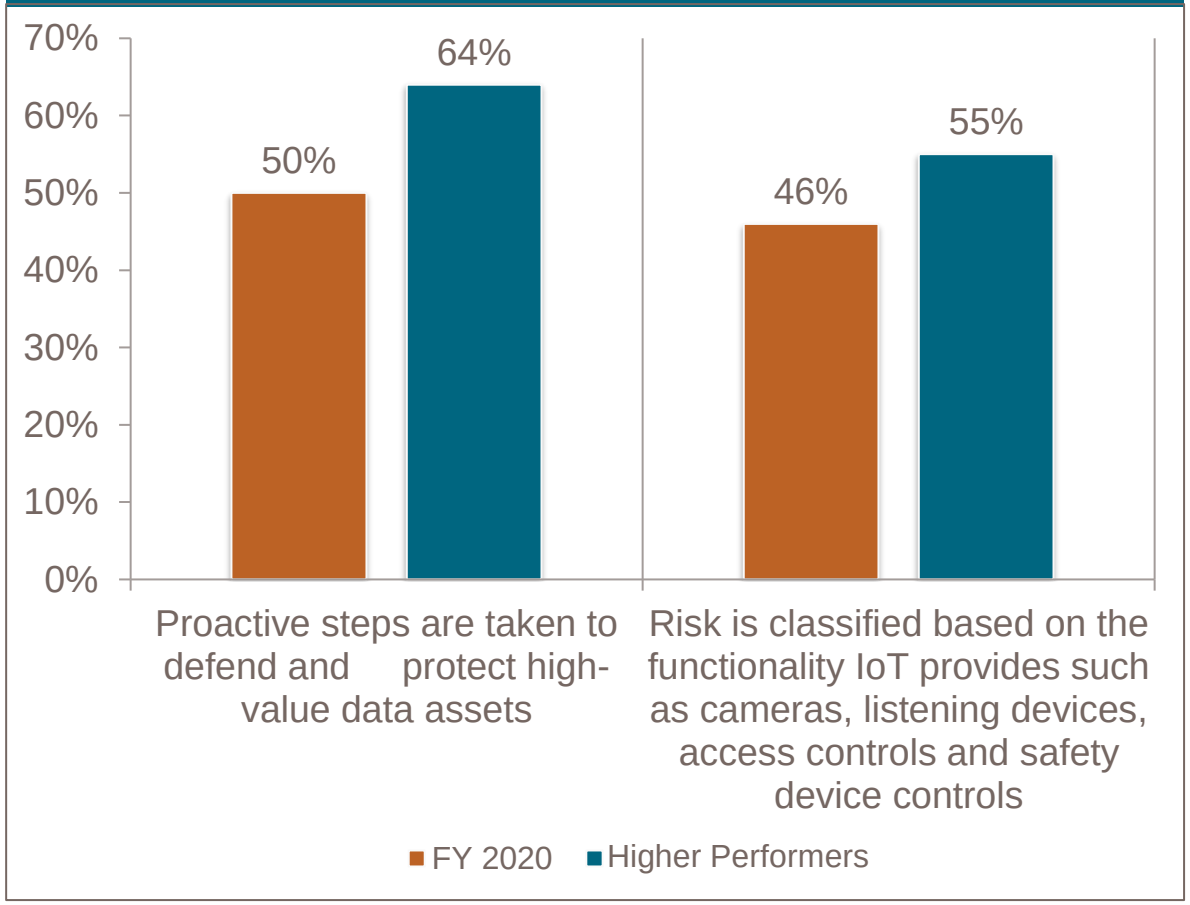


Company has an incident response plan for data breaches and security incidents involving third parties that includes responding to data breaches and security incidents that result from unsecured IoT

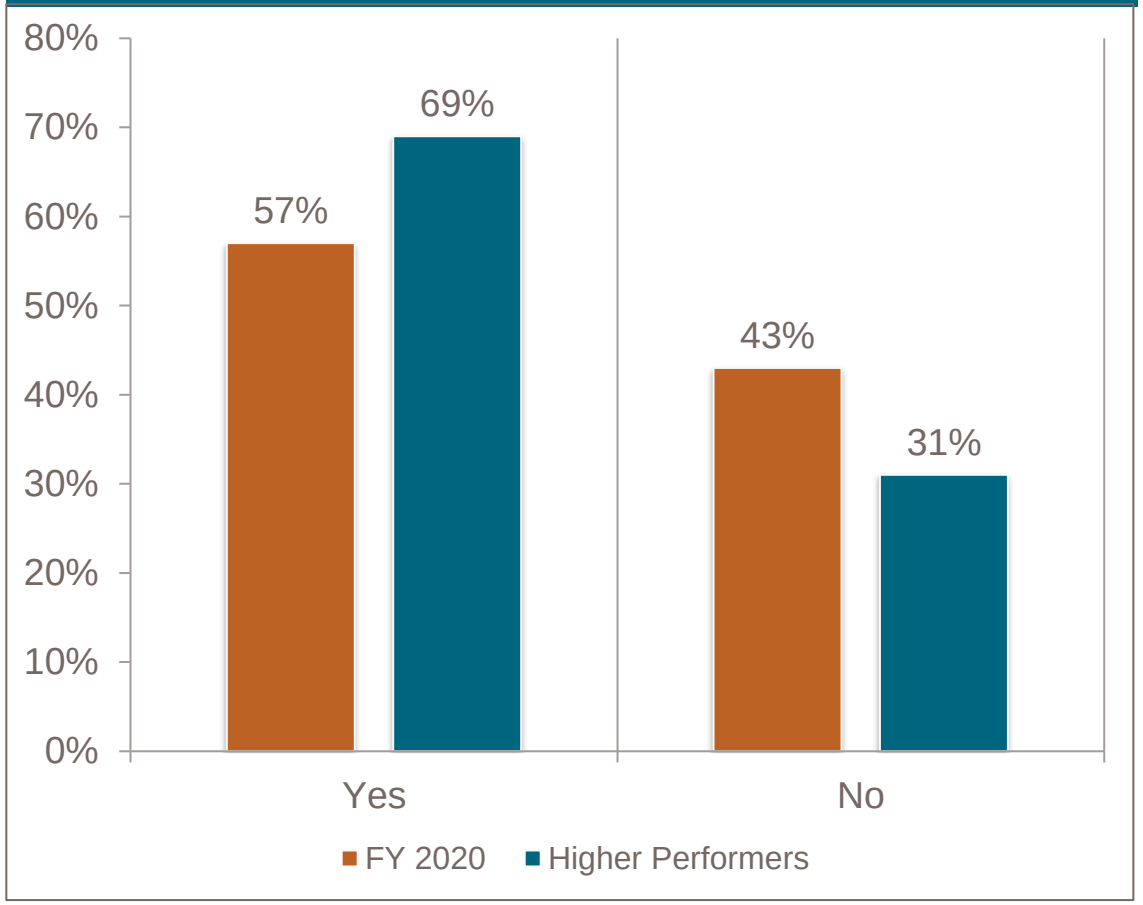


Risk Management

Steps taken to minimize IoT risk

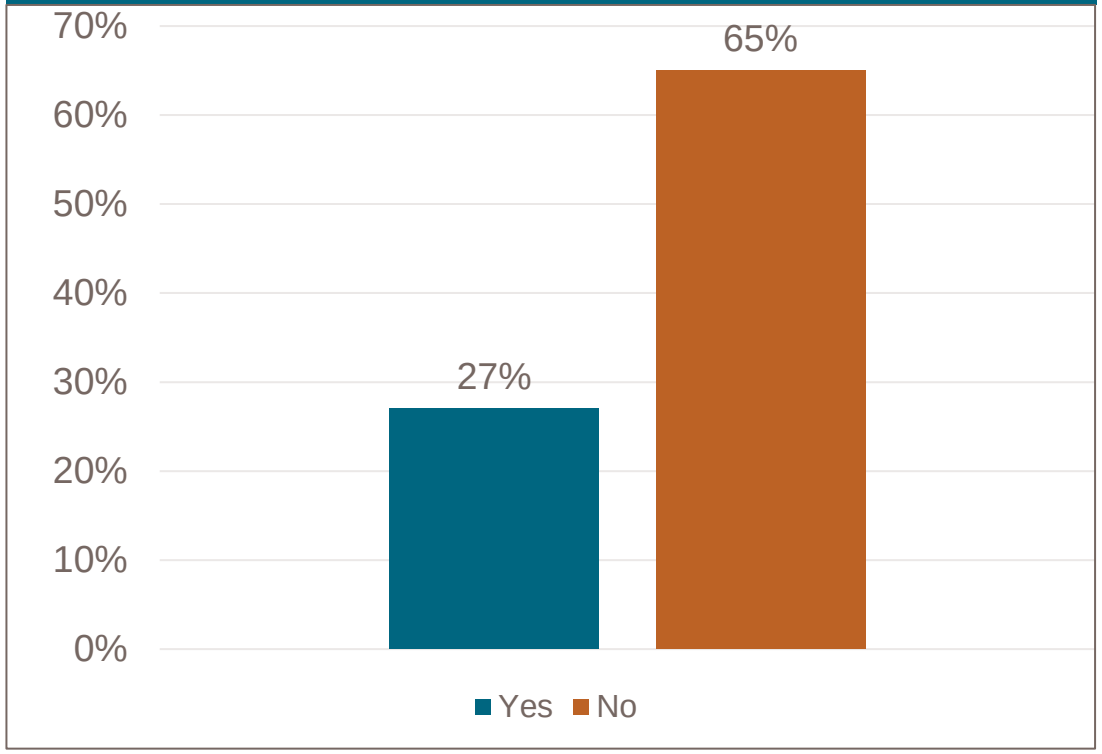


Organization has an approved IoT policy incorporating security considerations

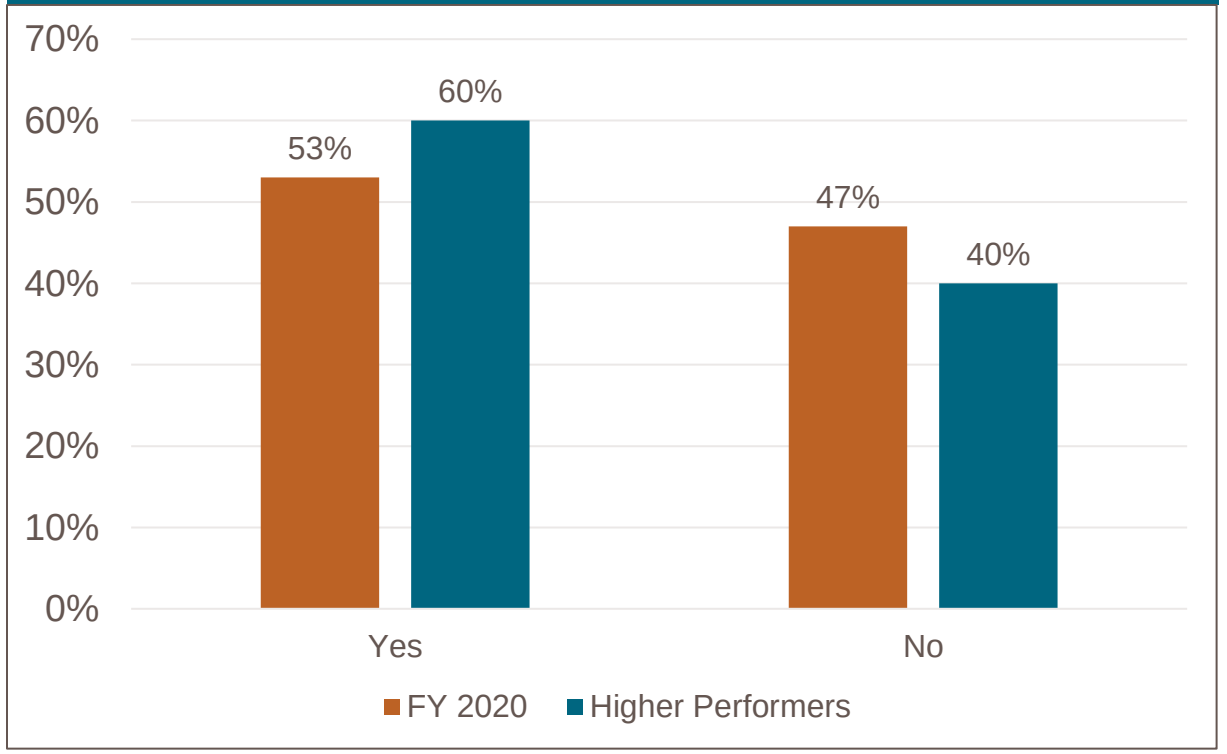


Third Party IoT Risk Management

Do you require third parties to identify and manage IoT devices connected to your network?

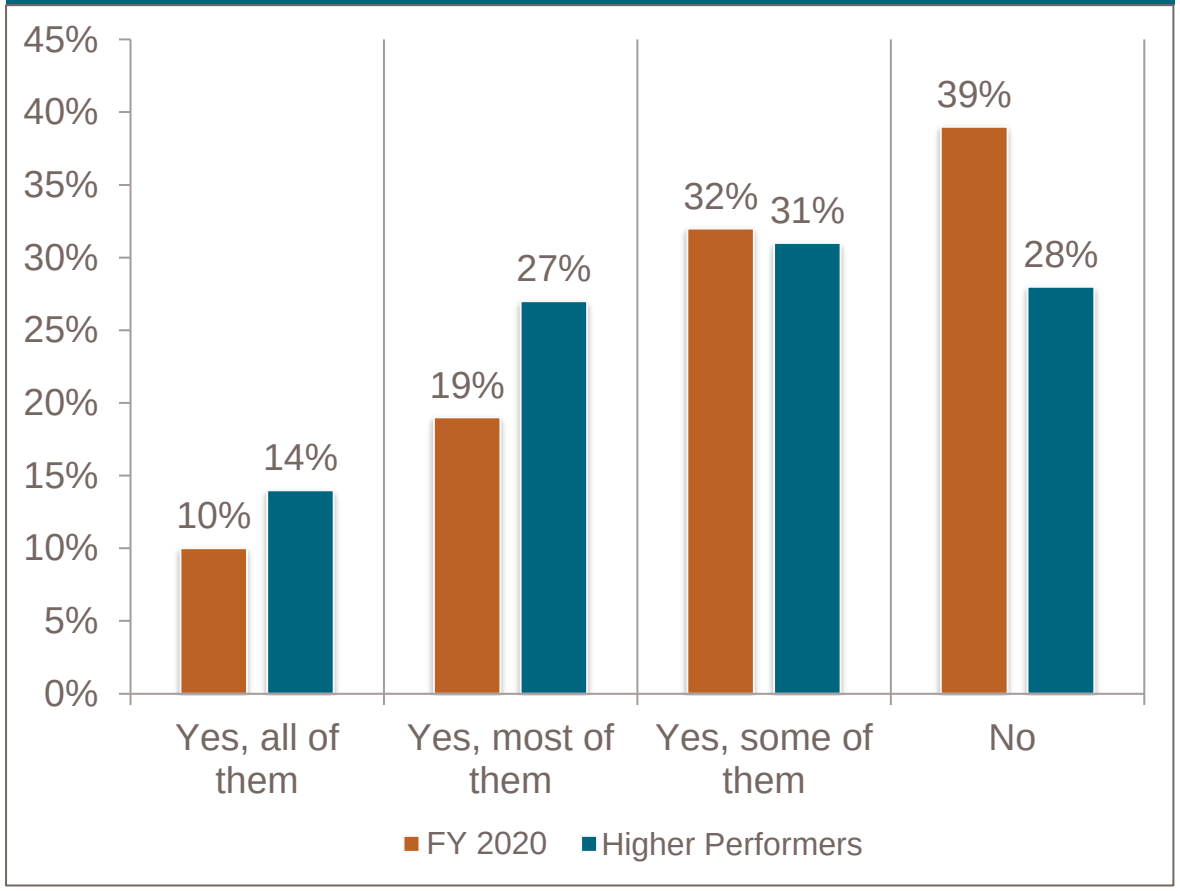


Does your organization consider and include compliance, standards and regulatory requirements related to IoT as part of its risk evaluation and selection of Third Parties?

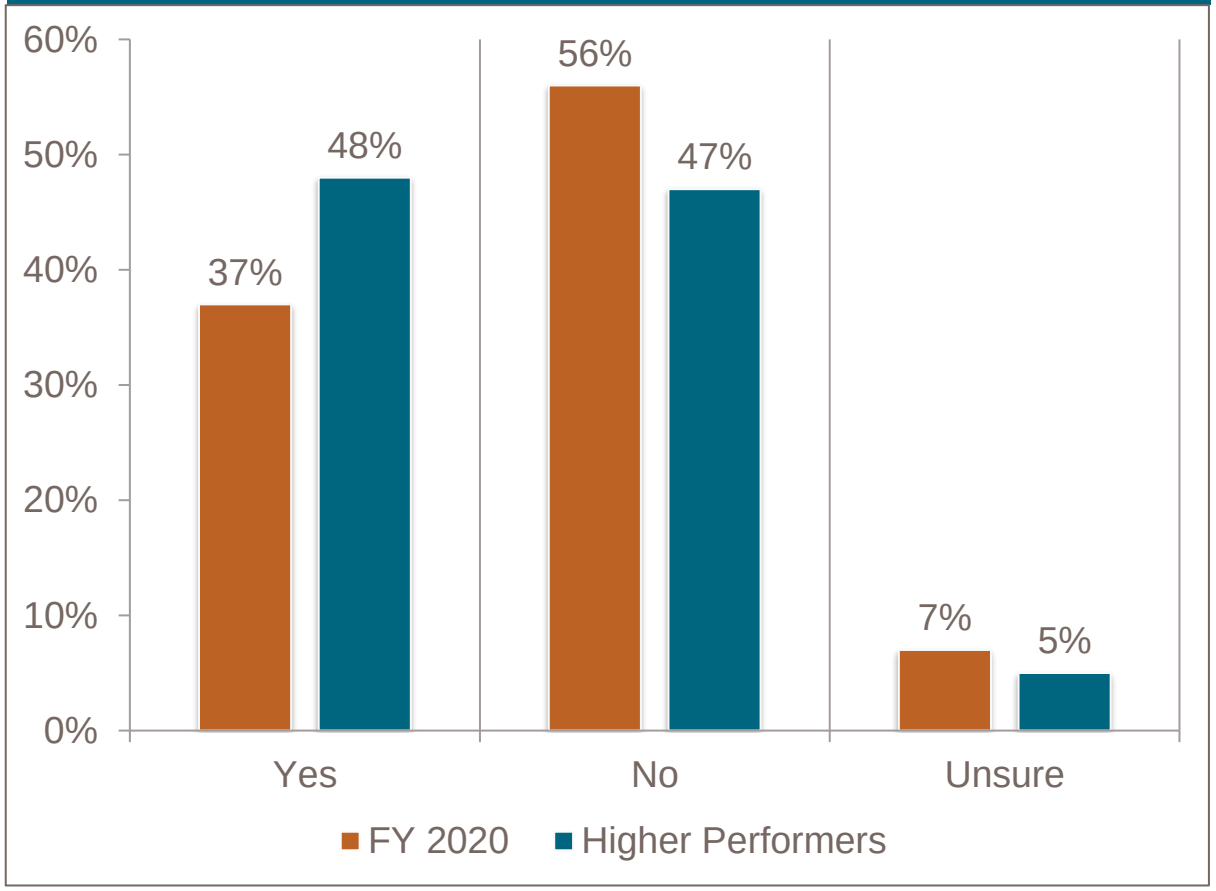


Asset Management

Aware of the network of physical objects in your company that are connected to the internet

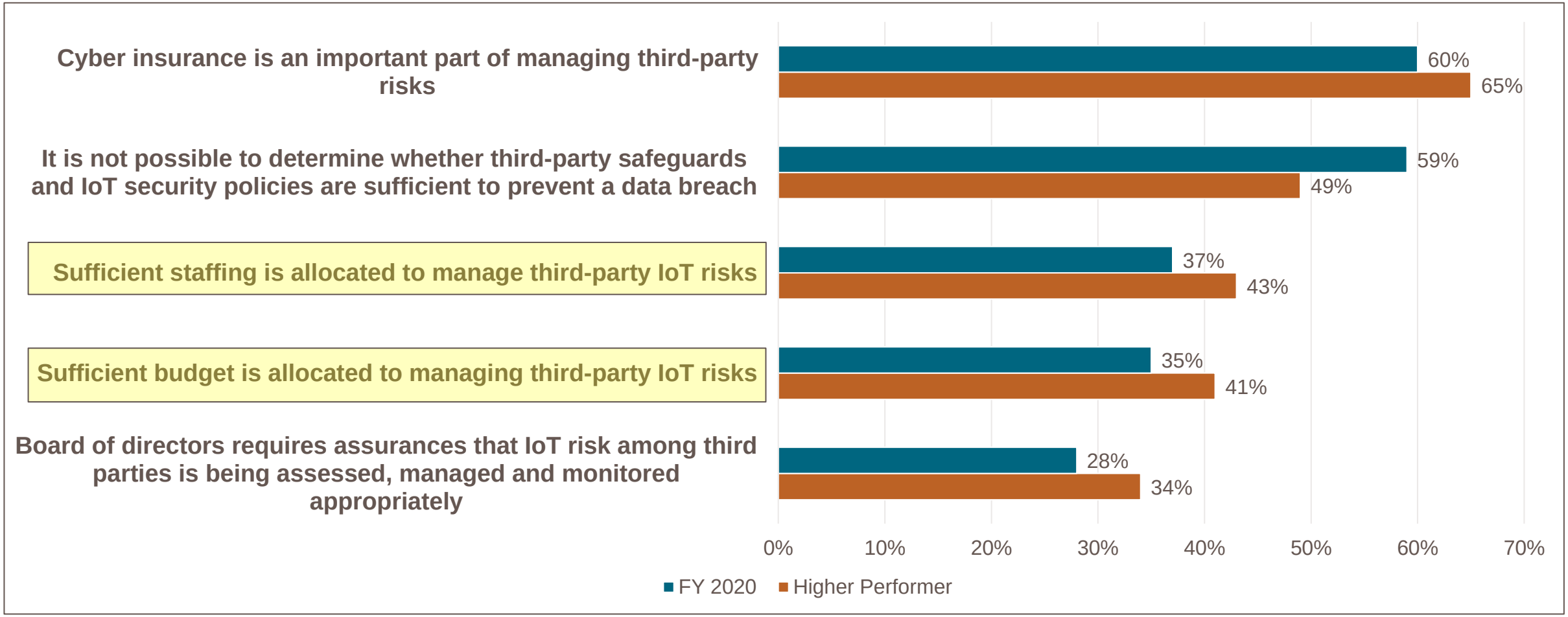


Has a formal network approval/entitlement process in place prior to attaching IoT and related applications to your network



Resource Allocation

Perceptions and steps taken to manage IoT and third party risk



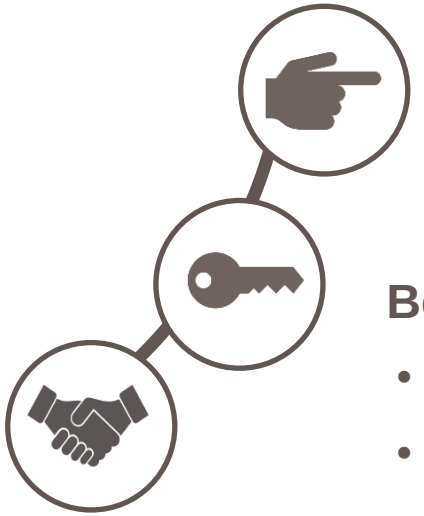
IoT – You Know The Risks Are Real …

- Personal Data Theft
- Key Fobs → Vehicle theft
- Safety System - Takeover
- ECU's, CAN's, OBD-II Dongel.s and Convivence Apps*
- Complexity of supply chains
- Limited patch and update capability
- IoT devices on legacy operating system

[Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT]

Recommendations

IoT To-Dos



Actions Needed:

- Accountability Asset Management
- Assess

Be Proactive:

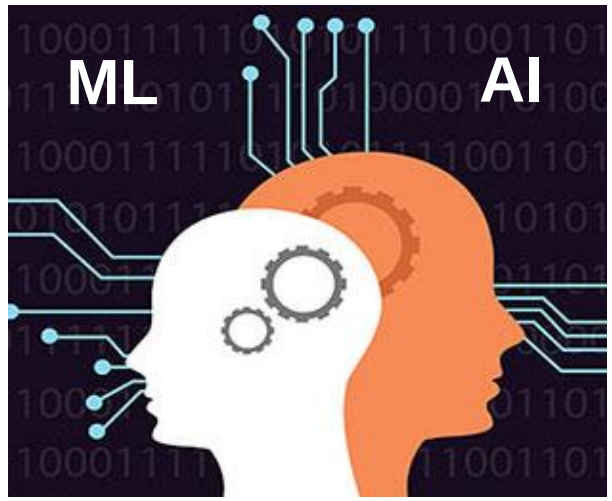
- Before connecting IoT
- Board and C-level disconnect closure

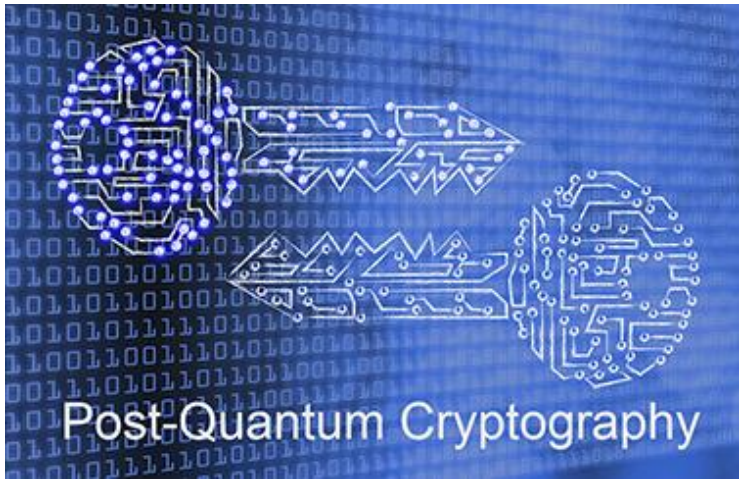
Collaborate, Continuously Monitor, Cooperate to:

- Ensure technologies/techniques used are secure – identify and mitigate IoT risk
- Demand that your CM solutions include IoT devices and applications
- Communicate risks, challenges, and success stories

- **Clearly define IoT accountabilities and policies**
- **Vet all IoT devices and applications against security standards**
- **Weed out unsecure devices**
- **Maintain a complete IoT inventory, and require third parties to do the same**
- **Place IoT devices on dedicated networks and monitor 24/7**
- **Include IoT in incident response plans**
- **Execute a complete IoT due diligence regime for third parties**

Final Thoughts – Emerging Technology Convergence





Resources

- **Shared Assessments**
  - *A New Roadmap for Third Party IoT Risk Management*, *in* collaboration with *Ponemon Institute*
  - *Enterprise Risk Management Technology Risk Briefing Paper*
  - *Vetting Vendors – IoT Risk Due Diligence Questions – Critical Awareness, Authority & Engagement*
- **Ponemon Institute**
  - *2020 Average Cost of a Data Breach* *plus other studies*
- **NIST**
  - *WHAT IS THE INTERNET OF THINGS (IOT) AND HOW CAN WE SECURE IT?*
- **ENISA**
  - *Guidelines for Securing the IoT – Secure Supply Chain for IoT*
- **USENIX**
  - *Plug-N-Pwned: Comprehensive Vulnerability Analysis of OBD-II Dongles as A New Over-the-Air Attack Surface in Automotive IoT*
- **Palo Alto Networks**
  - *2020 Unit 42 IoT Threat Report*

About Shared Assessments

Shared Assessments is uniquely positioned and focused on process and development of robust enterprise-wide Third Party Risk Management (TPRM) solutions and standardized resources for critical advancement of TPRM controls in an otherwise fractured market.

We believe that the power of many protects and builds trusted communities.

Our purpose is to harness the collective intelligence of a diverse membership to create a more secure and resilient world.

About Ponemon Institute

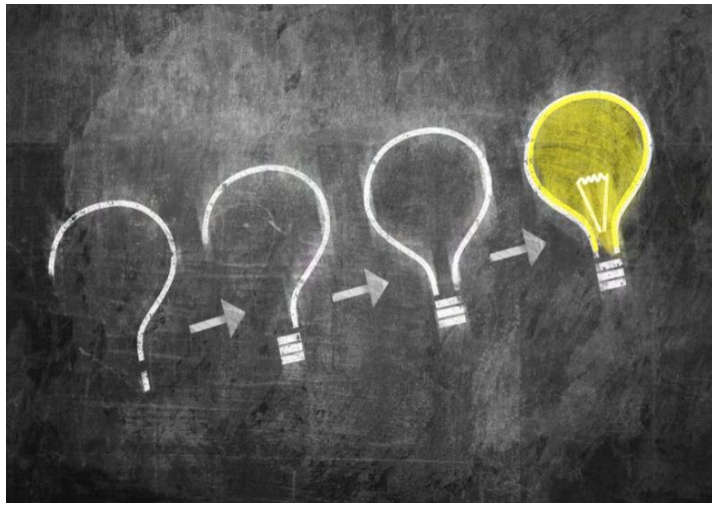
Ponemon Institute was founded in 2002 by Dr. Larry Ponemon and Susan Jayson. The Institute is dedicated to independent research and education that advances the responsible use of information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the security of information assets and the IT infrastructure.

Organizations engage Ponemon Institute to conduct studies on topics that support their thought leadership and marketing objectives. The Institute is best known for its annual Cost of Data Breach sponsored by IBM and the annual Encryption Trends study now sponsored by n-Cipher. Other topics, to name a few, include the cost of insider risks, endpoint security, the economics and effectiveness of security operation centers, how to prepare for a data breach, the importance of prevention in the cybersecurity lifecycle, application security, vulnerability management, third parties and the IoT risk and privileged access management.

Thank You

Stay Safe

The Santa Fe Group,
Shared Assessments Program
3 North Chamisa Drive, Suite 2
Santa Fe, NM 87508 USA
(917) 279-2229
www.sharedassessments.org
charlie@santa-fe-group.com



Alvarez & Marsal
600 Madison Avenue, 8th Floor
New York, NY 10022
Global Cyber Risk Services
(917) 693-9700
rgrillo@alvarezandmarsal.com

Ponemon Institute
2308 US 31 North
Michigan HQ: 2308 US 31 N.
Traverse City, MI 49686 USA
800-887-3118
http://www.ponemon.org
research@ponemon.org

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- Real-time Intelligence Sharing
- Intelligence Summaries
- Regular intelligence meetings
- Crisis Notifications
- Member Contact Directory
- Development of Best Practice Guides
- Exchanges and Workshops
- Tabletop exercises
- Webinars and Presentations
- Annual Auto-ISAC Summit Event

To learn more about Auto-ISAC Membership or Partnership, please contact Auto-ISAC! fayefrancy@automotiveisac.com

Auto-ISAC Partnership Programs

Strategic Partner | **Community Partners**

Solutions Providers

For-profit companies that sell connected vehicle cybersecurity products & services.

Examples: Hacker ONE, IOActive, Karamba, Grimm

Associations

Industry associations and others who want to support and invest in the Auto-ISAC activities.

Examples: Auto Alliance, ATA, ACEA, JAMA

Affiliations

Government, academia, research, non-profit orgs with complementary missions to Auto-ISAC.

Examples: NCI, DHS, NHTSA, Colorado State

Community

Companies interested in engaging the automotive ecosystem and supporting & educating the community.

Examples: Sponsors for key events, technical experts, etc.

INNOVATOR
Paid Partnership

- Annual investment and agreement
- Specific commitment to engage with ISAC
- In-kind contributions allowed
- Must be educational provide awareness

NAVIGATOR
Support Partnership

- Provides guidance and support
- Annual definition of activity commitments and expected outcomes
- Provides guidance on key topics / activities
- Supports Auto-ISAC

COLLABORATOR
Coordination Partnership

- "See something, say something"
- May not require a formal agreement
- Information exchanges-coordination activities
- Information Sharing / research & development

BENEFACTOR
Sponsorship Partnership

- Participate in monthly community calls
- Sponsor Summit
- Network with Auto Community
- Webinar / Events

Current Partnerships

Many organizations engaging

INNOVATOR
Strategic Partnership (12)

ArmorText

Celerium

Cybellum

Ernst and Young

FEV

GRIMM

HackerOne

Karamba Security

Pen Testing Partners

Red Balloon Security

Regulus Cyber

Saferide

Trillium Secure

NAVIGATOR
Support Partnership

AAA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR
Coordination Partnership

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA - DoCommerce
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsch College

BENEFACTOR
Sponsorship Partnership

2019 Summit Sponsors-
Argus
Arxan
Blackberry
Booz Allen Hamilton
Bugcrowd
Celerium
Cyber Future Foundation
Deloitte
GM
HackerOne
Harman
IOActive
Karamba Security
Keysight
Micron
NXP
PACCAR
Recorded Future
Red Balloon Security
Saferide
Symantec
Toyota
Transmit Security
Upstream
Valimail

Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency

Building Resiliency Across the Auto Industry

Thank you!

рахмат
danke
謝謝
ngiyabonga
شكراً جزيلاً
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
welalin
tack
mahalo
спасибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
tapadh leat
kiitos
dankie
thank you
gracias
хвала
nanni
nandri
dhanyavad
mauruuru
köszönöm
asante
manana
tenki
bedankt
bayarlalaa
gràçie
hvala
dankon
aciu
akun
obrigada
enkosi
djiere dieuf
tau
mochchakkeram
murakoze
dziękuję
дякую
mamnun
chnorakaloutioun
gratias ago
gràcies
sulpáy
go raibh maith agat
chokrane
sobodi
dēkuji
sagolun
sukriya
kop khun krap
taiku
obrigado
mèsi
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
trugarez
didi madloba
najis tuke
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
mercê
мерси
kam sah hamnida
rahmat
ευχαριστώ
তোমাকে ধন্যবাদ
감사합니다
xièxie
merci

Our contact info

Faye Francy
Executive Director

20 F Street NW, Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

Sharmila Khadka
Executive Organizational Secretary

20 F Street NW, Suite 700
Washington, DC 20001
sharmilakhadka@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

www.automotiveisac.com
@auto-ISAC