RESEARCH

IoT and IIoT Security Survey

What More Connected Devices Mean for Industrial Security

MARCH 2021

FOUNDATIONAL CONTROLS FOR
SECURITY, COMPLIANCE & IT OPERATIONS

Research Goal

The primary research goal was to understand current approaches, challenges, and opinions about security of connected devices in enterprise environments including ICS, IIoT, and consumer IoT.

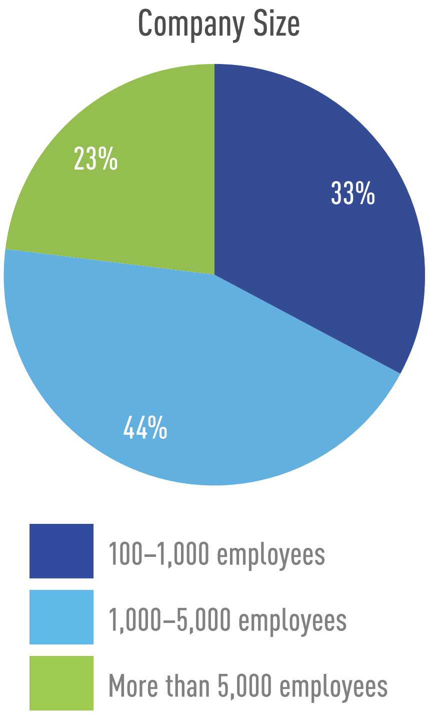
Methodology

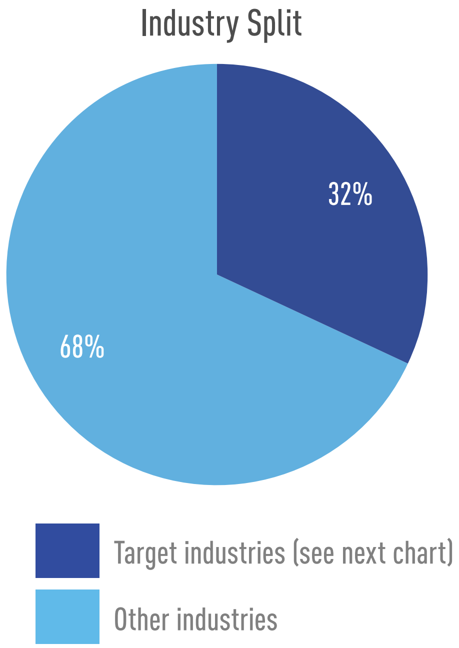
Independent sources of security professionals were invited to participate in an online survey. A variety of questions were asked on topics related to IoT. Responses were captured between March 3 and March 10, 2021.

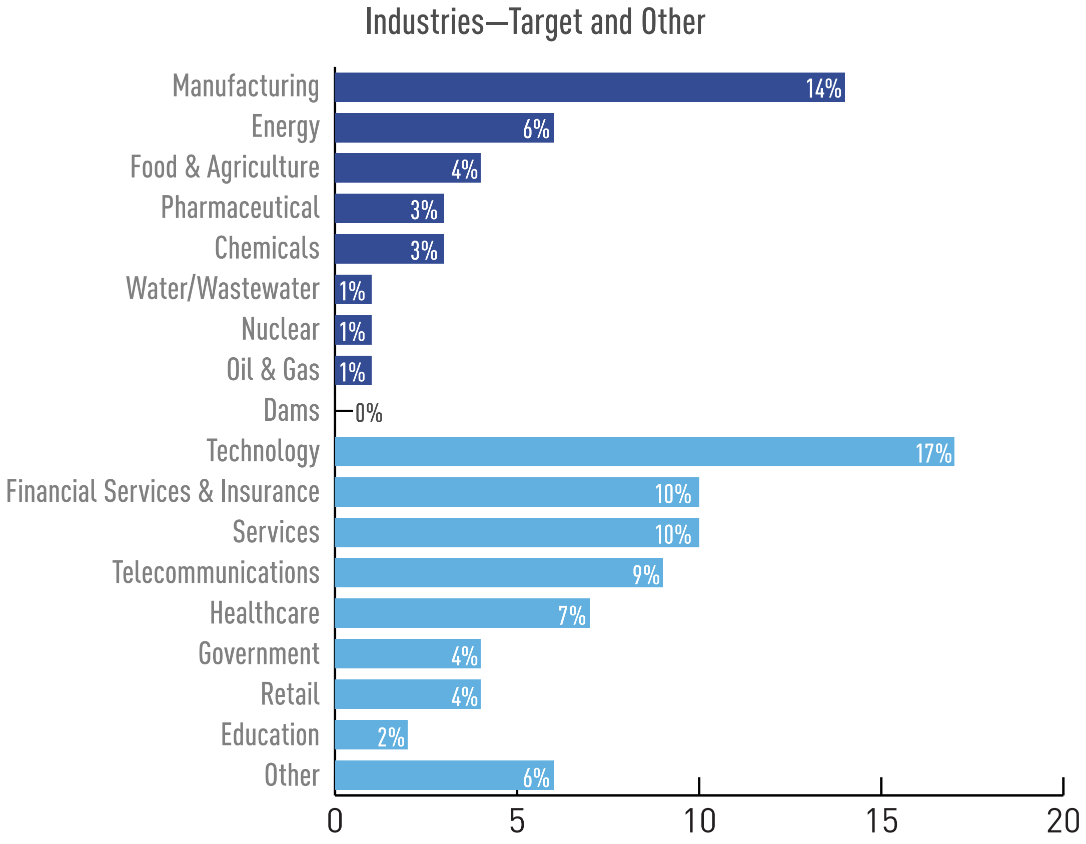
Participants

A total of 312 qualified individuals completed the survey. All had direct responsibility for the security of IoT devices at a company in the United States or Europe with at least 100 employees.

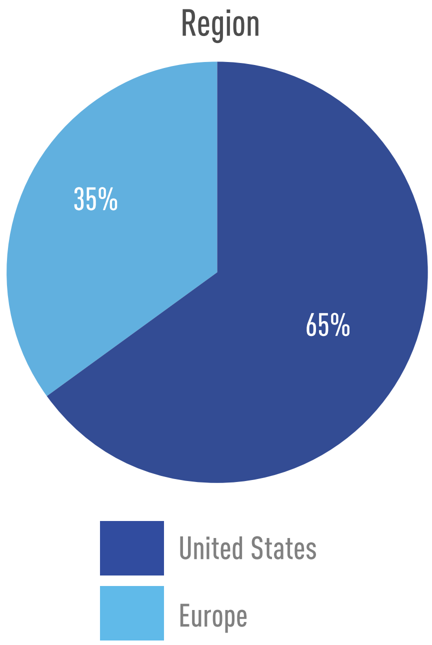
COMPANIES REPRESENTED

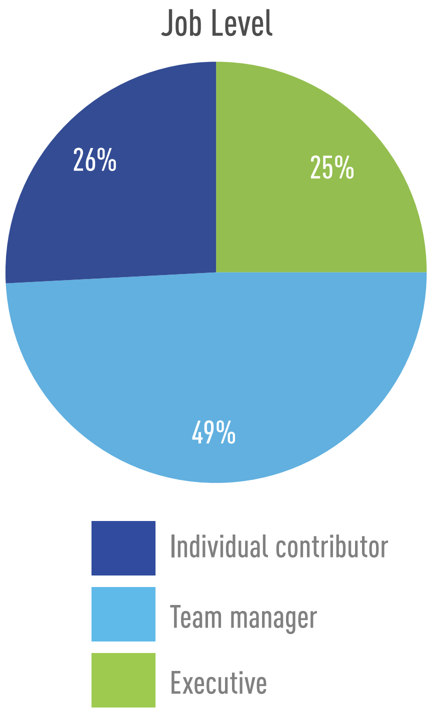


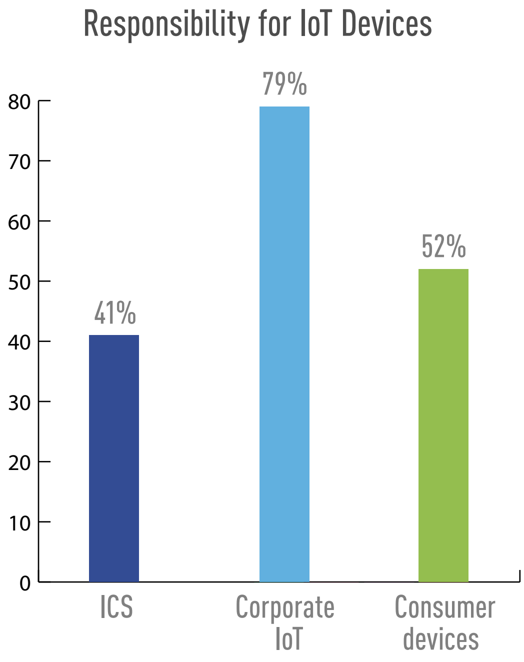




INDIVIDUALS REPRESENTED







Defining IoT

In this study, IoT (Internet of Thing) devices referred to any device that is able to connect to the internet, including:

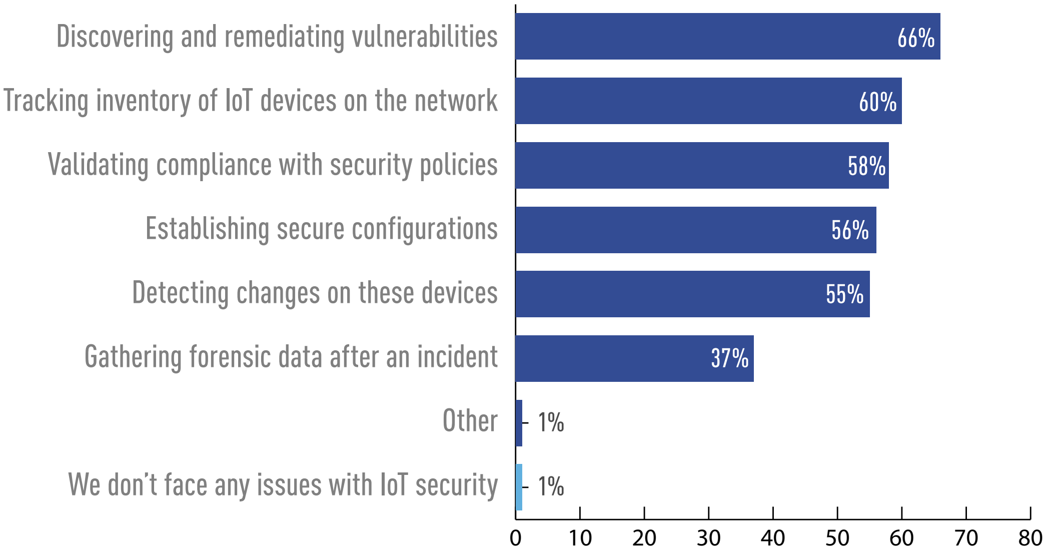
- Consumer devices such as smart watches, digital health monitors and connected home products (refrigerator, speakers, smart locks, etc.)
- Corporate IoT systems (smart buildings, logistics trackers, etc.)
- Industrial control systems (ICS) such as factory automation, power generation and machinery

In this study, IoT does *not* include traditional connected devices such as laptops, servers, routers, or mobile phones.

All participants read and agreed to this definition.

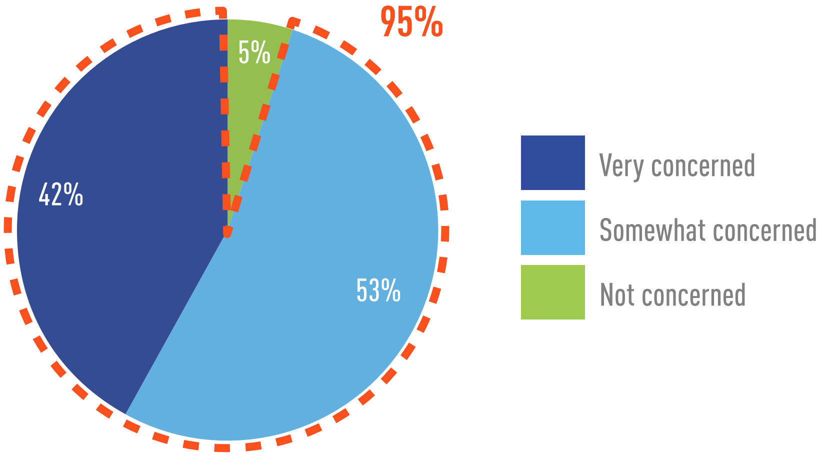
99% OF SECURITY PROFESSIONALS REPORT CHALLENGES WITH THE SECURITY OF THEIR IoT AND IIoT DEVICES

What challenges does your company face with the security of IoT and IIoT devices? Choose all that apply.



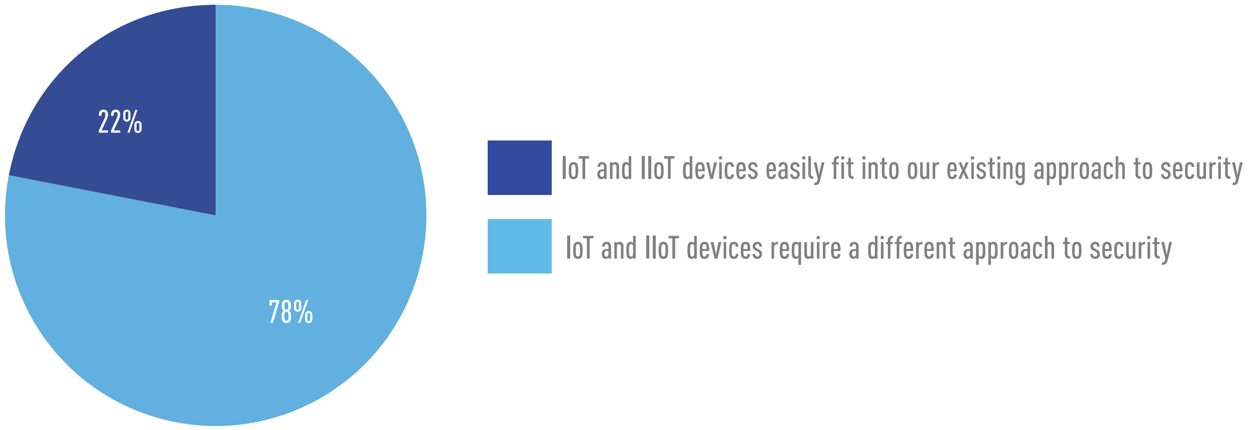
95% ARE CONCERNED ABOUT THE SECURITY RISKS ASSOCIATED WITH THEIR CONNECTED DEVICES

How concerned is your company about the security risk of IoT and IIoT devices?



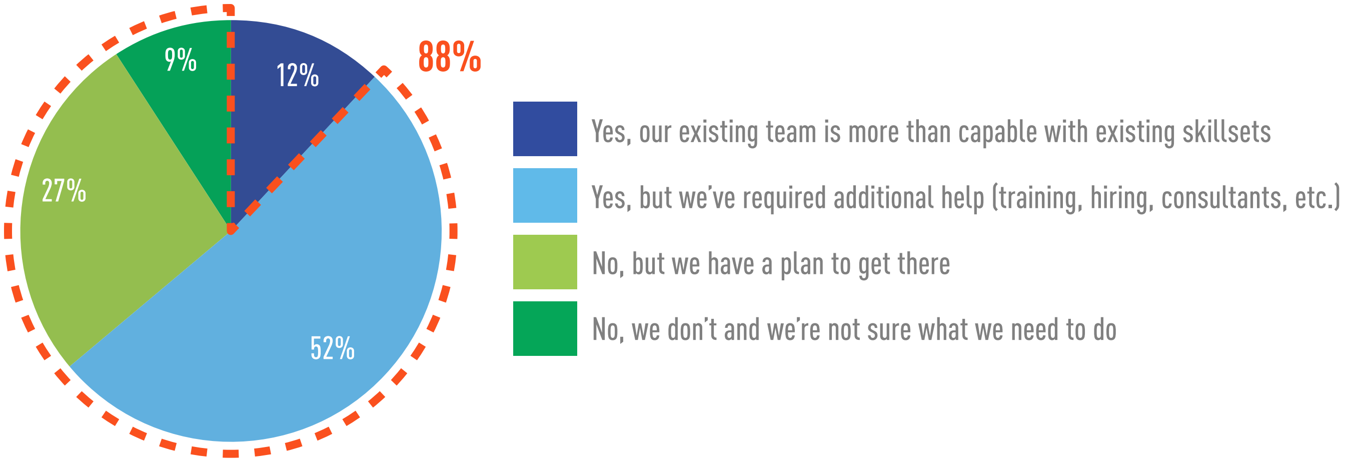
MORE THAN THREE QUARTERS SAID THAT IOT AND IIOT DEVICES DO NOT EASILY FIT INTO THEIR EXISTING SECURITY APPROACH

Which of the following statements best represents your personal security philosophy?



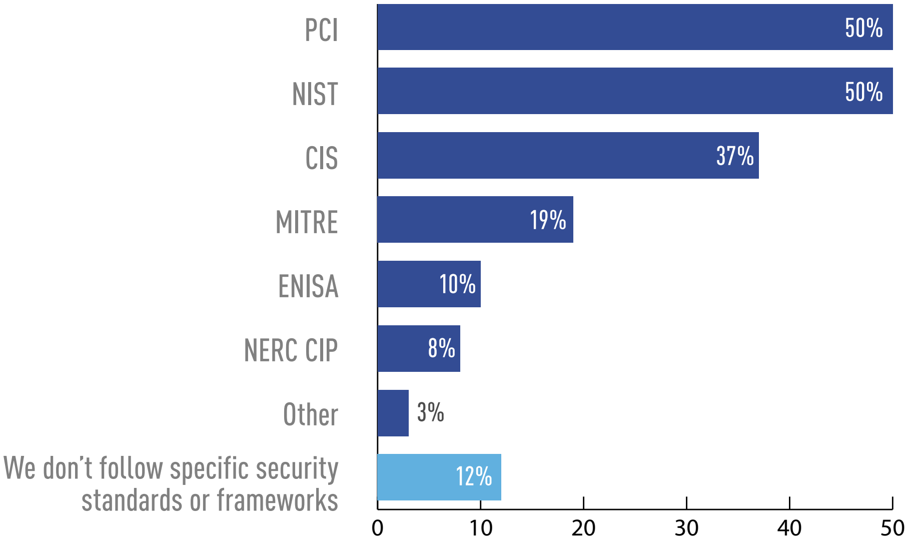
88% REQUIRED (OR STILL REQUIRE) ADDITIONAL HELP FOR IoT AND IIoT SECURITY NEEDS

In your opinion, is your team adequately resourced for the security needs of IoT and IIoT devices across your company?



88% FOLLOW SOME KIND OF SECURITY STANDARD OR FRAMEWORK

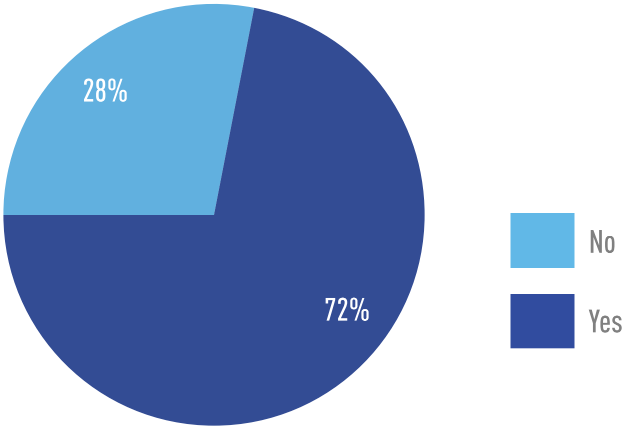
What security standards or frameworks does your company follow? Choose all that apply.



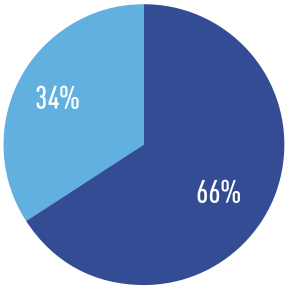
Other
Most common: ISO
Also HIPAA; HITRUST; CSA; native Dutch

AND MOST OF THOSE THAT FOLLOW SECURITY STANDARDS ARE AUDITED FOR THEM

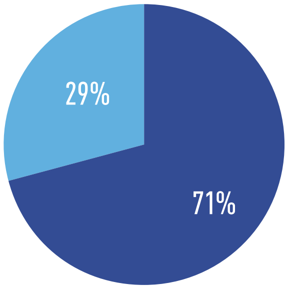
Is your company audited for compliance with these security standards?



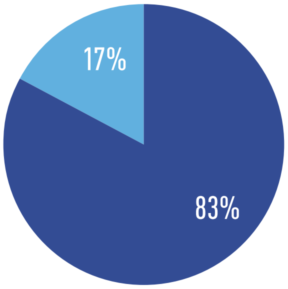
By Company Size (# of employees)



100–1,000 Employees



1,000–5,000 Employees

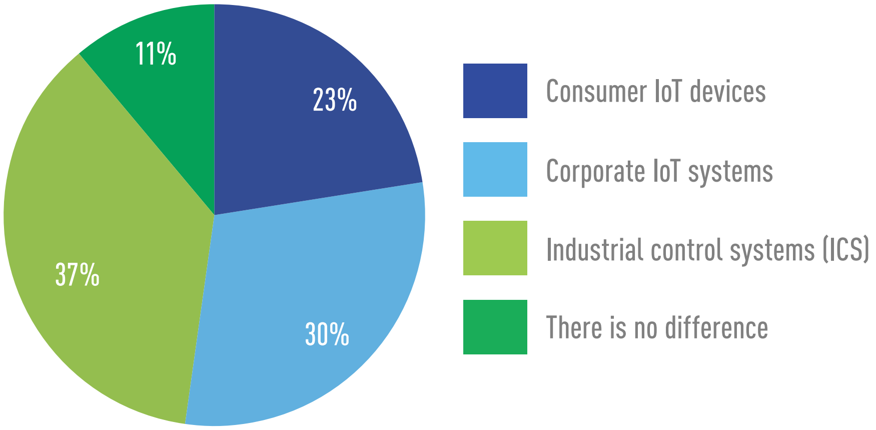


More than 5,000 Employees

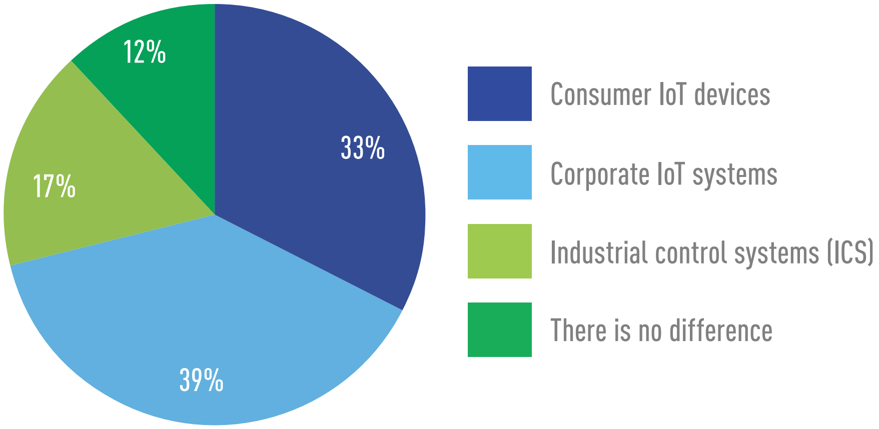
INDUSTRIAL PROFESSIONALS ACROSS TARGET INDUSTRIES* BELIEVE THEY WOULD BENEFIT FROM EXPANDED ICS SECURITY STANDARDS

What types of devices do you think would benefit *most* from expanded security standards? Choose the one answer that most closely applies.

Target industries*



Other industries

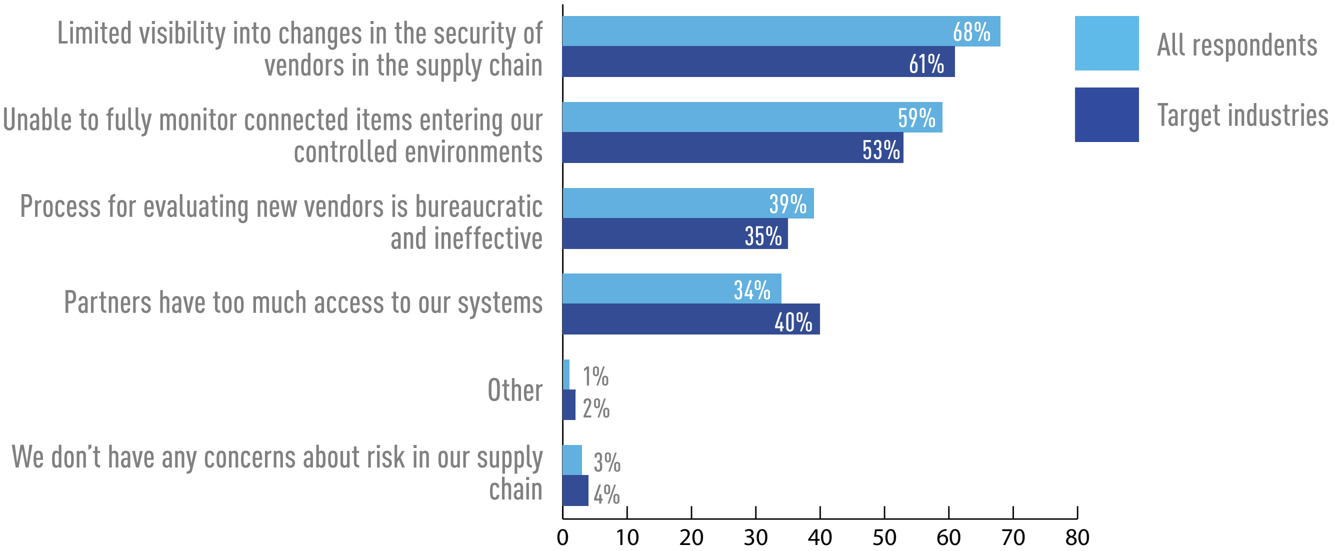


*Manufacturing, energy, farm & agriculture, oil & gas, pharmaceutical, chemical, nuclear, and water/wastewater

97% OF ALL RESPONDENTS HAVE CONCERNS ABOUT SUPPLY CHAIN SECURITY

What concerns do you have about security risks within your supply chain?

Choose all that apply.



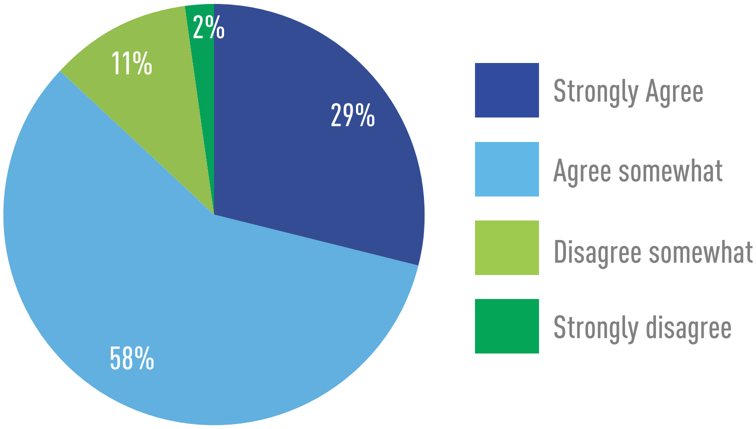
Other

"Vendor is compromised but not aware they've been breached, à la SolarWinds."

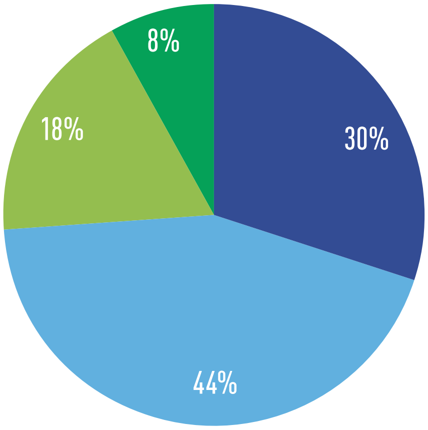
87% AGREE THAT EXISTING IOT SECURITY GUIDELINES PUT THEIR SUPPLY CHAIN SECURITY AT RISK

Please indicate your agreement with each of the following statements.

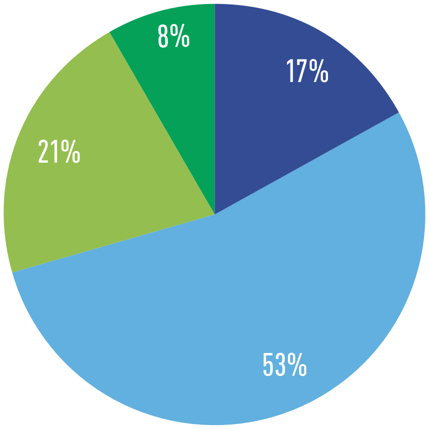
I worry about security risk to our supply chain based on existing IIoT security guidelines



The government needs to step up and deliver consistent security guidelines for connected devices

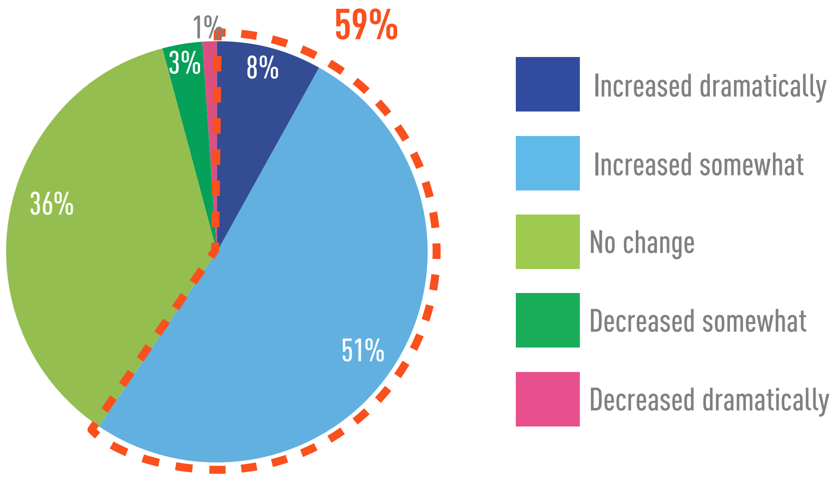


It feels like our business leaders want us to connect everything to the internet



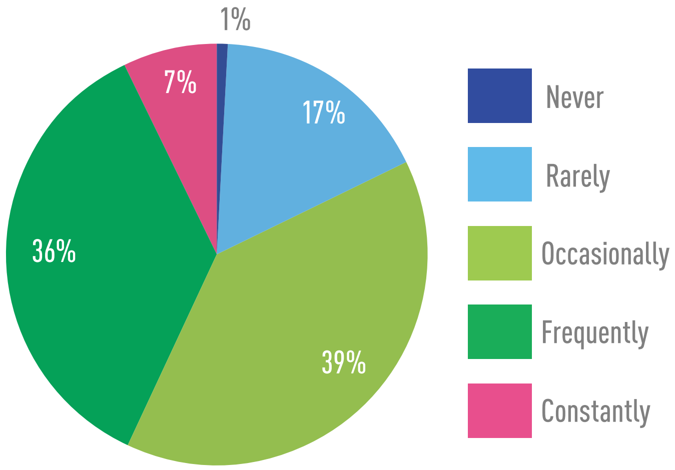
59% REPORT THAT BUDGET FOR MANAGING SUPPLY CHAIN SECURITY INCREASED IN THE PAST YEAR

In the past year, how has your security team's budget for managing the security of your company's supply chain changed?



99% REPORT THAT THEIR SECURITY TEAMS DO REFUSE REQUESTS TO CONNECT DEVICES; 43% SAY THEY OFTEN DO

How often does your security team refuse a request from an employee to connect a device to your corporate network?



Tripwire is the trusted leader for establishing a strong cybersecurity foundation. We protect the world's leading organizations against the most damaging cyberattacks, keeping pace with rapidly changing tech complexities to defend against ever-evolving threats for more than 20 years. On-site and in the cloud, our diverse portfolio of solutions find, monitor and mitigate risks to organizations' digital infrastructure—all without disrupting day-to-day operations or productivity. Think of us as the invisible line that keeps systems safe. **Learn more at tripwire.com**

The State of Security: **News, trends and insights at tripwire.com/blog**
Connect with us on LinkedIn, Twitter and Facebook