



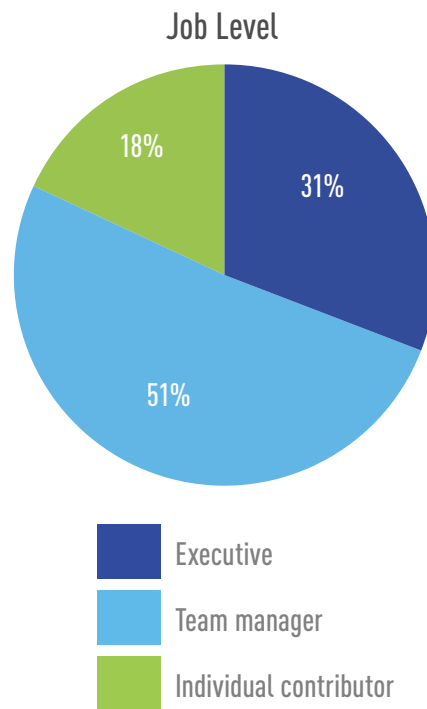
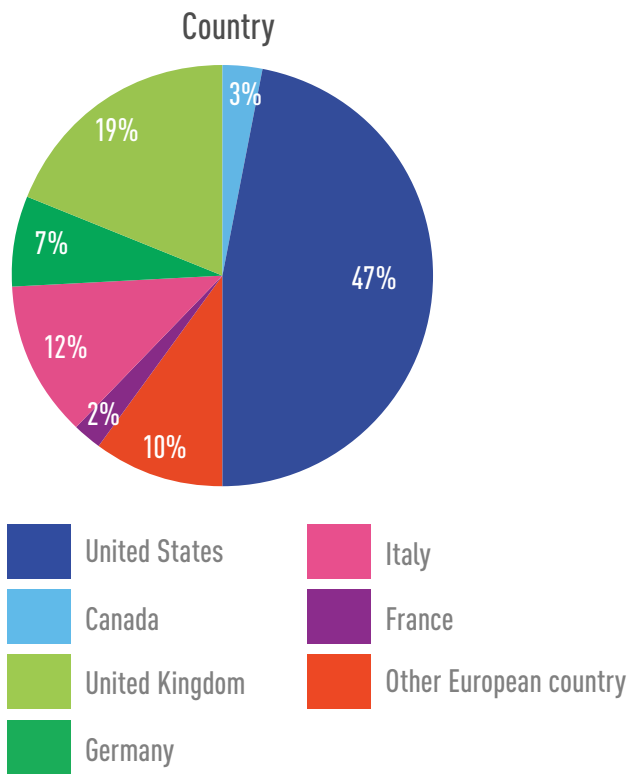
Retail Security Survey

December 2020

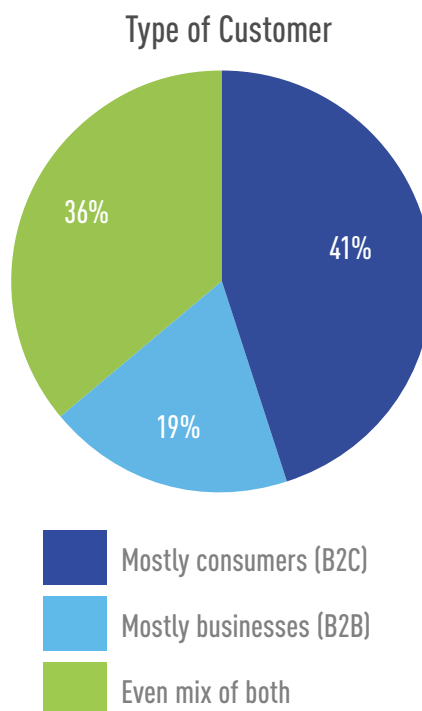
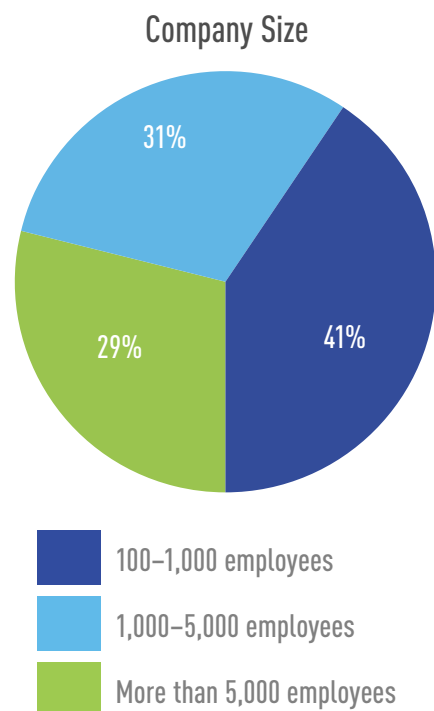
The retail industry always has to make special preparations for the holiday season. That was especially the case this year. With Covid-19 disrupting shopping behaviors and creating a surge in online shopping, security teams at these retail organizations have had to make adjustments as well.

Tripwire partnered with Dimensional Research to understand how retail organizations are adapting their cybersecurity programs in the face of the pandemic and increased online shopping. They conducted the survey in November 2020 with a total of 203 security professionals working in the retail industry. This report summarizes findings about their 2020 holiday shopping preparations and their current state of cybersecurity capabilities.

INDIVIDUALS REPRESENTED

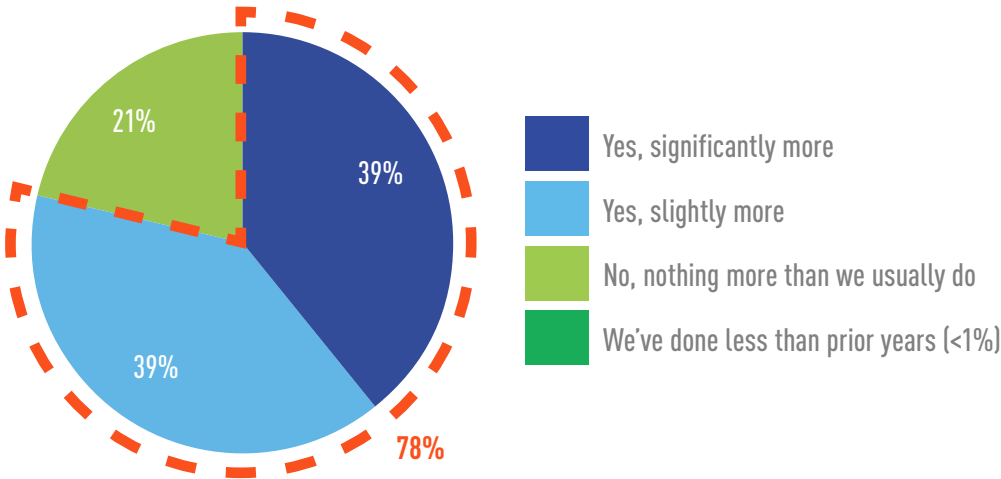


COMPANIES REPRESENTED

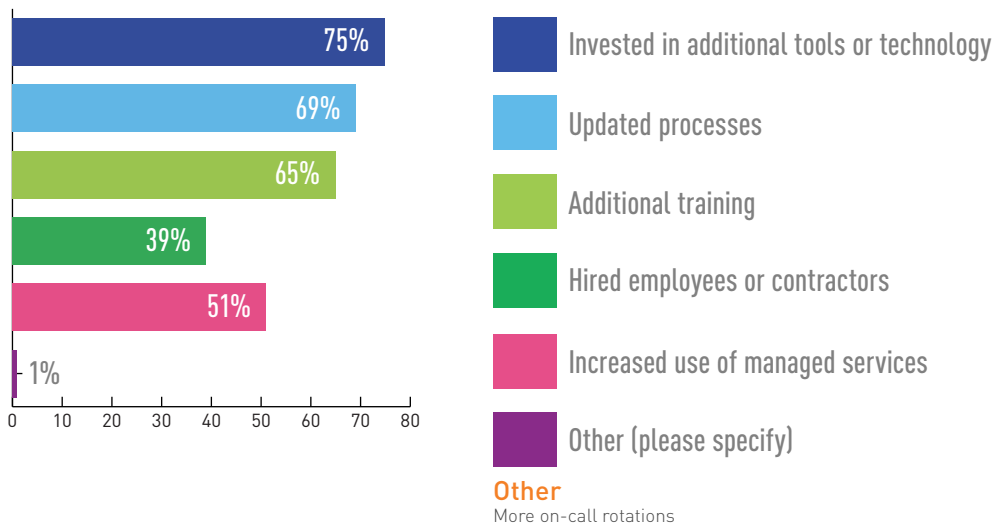


MORE THAN THREE-QUARTERS (78%) HAVE TAKEN ADDITIONAL IT SECURITY PRECAUTIONS FOR 2020

Compared to prior years, has your IT security team taken additional precautions for the 2020 holiday shopping season?

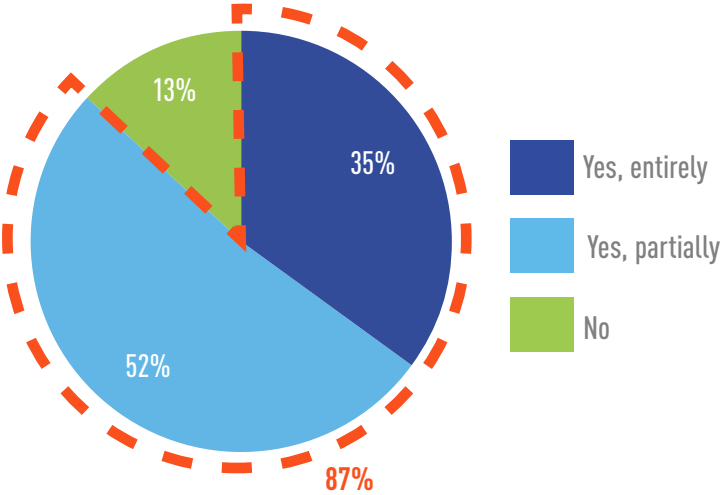


What additional precautions has your IT security team made for the 2020 holiday shopping season compared to prior years? Choose all that apply.



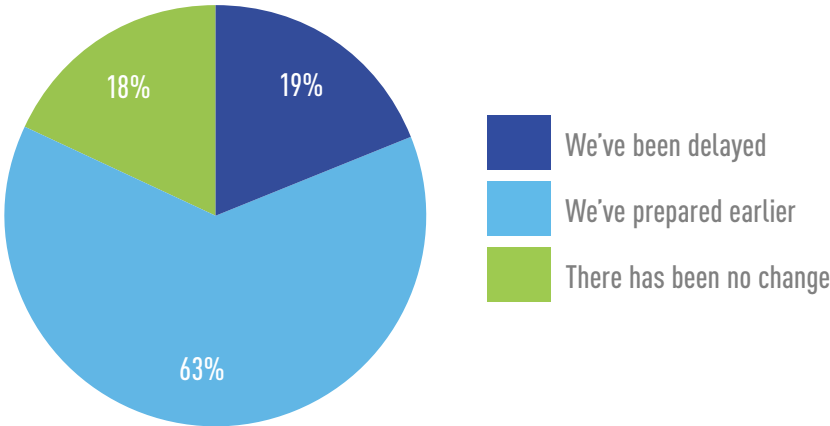
OF THOSE, 87% SAID THIS WAS SPECIFICALLY RELATED TO THE PANDEMIC.

Are the additional security precautions your IT security team made for the 2020 holiday shopping season a result of Covid-19?



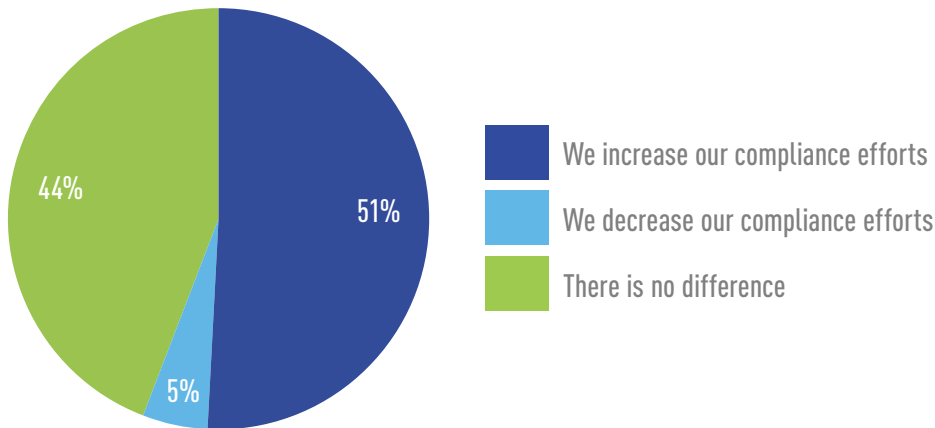
IT SECURITY TEAMS TYPICALLY PREPARED EARLIER FOR HOLIDAY SHOPPING IN 2020

How has your IT security team's timeline for preparing for holiday shopping changed for 2020 compared to prior years?



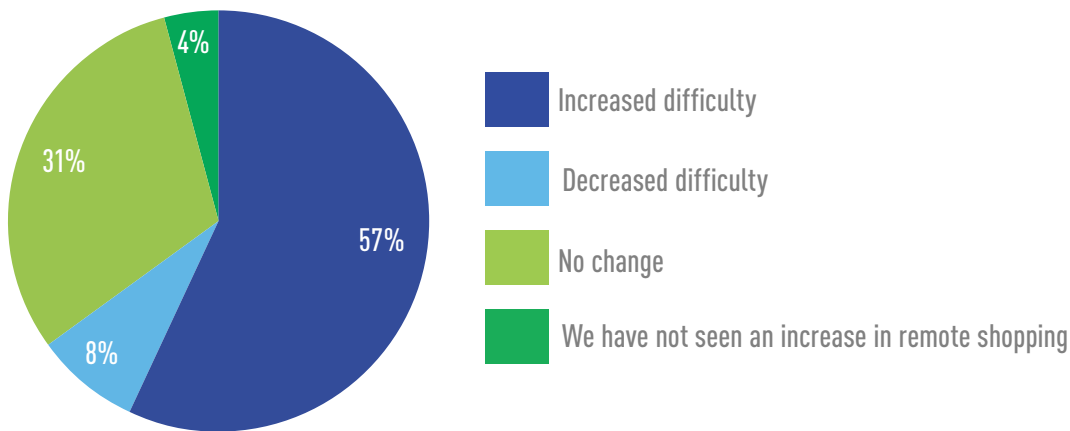
OVER HALF ALSO RAMP UP SECURITY-RELATED COMPLIANCE EFFORTS FOR THE HOLIDAY SEASON.

How does the holiday shopping season impact your IT security team's compliance efforts (PCI, SOX, GDPR, etc.)?

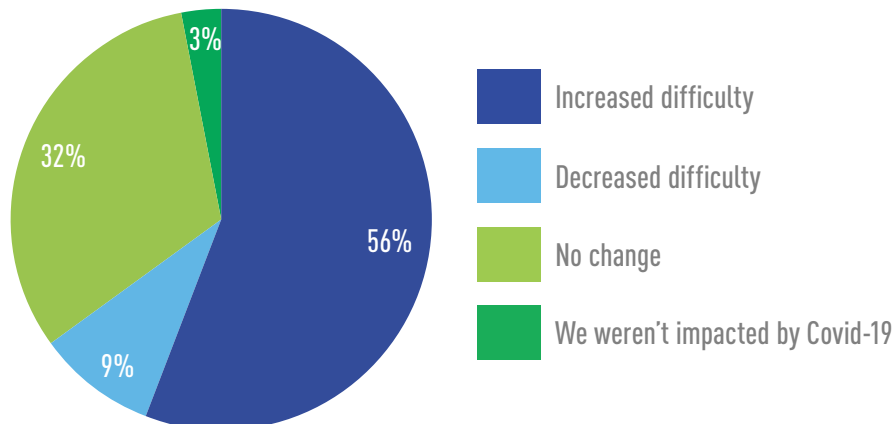


INCREASED ONLINE SHOPPING AND COVID-19 IMPACTS HAVE MADE SECURITY MORE DIFFICULT FOR MANY RETAILERS

How has 2020's increase in remote shopping impacted *security* efforts?

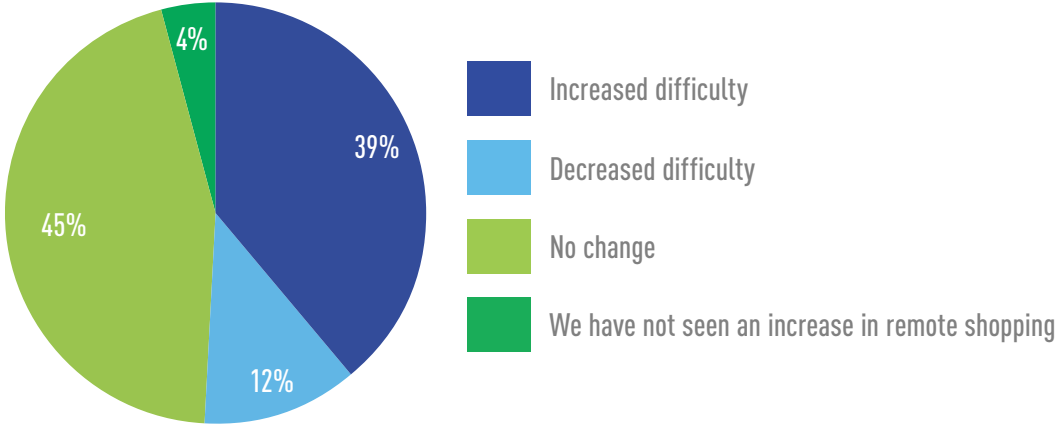


How have factors related to Covid-19 impacted *security* efforts in 2020?

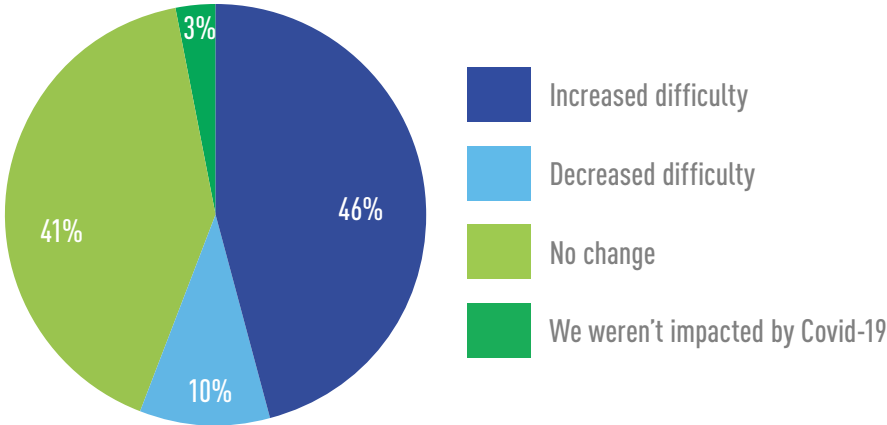


INCREASED ONLINE SHOPPING AND COVID-19 IMPACTS HAVE MADE COMPLIANCE MORE DIFFICULT FOR MANY RETAILERS

How has 2020's increase in remote shopping impacted *compliance* efforts?

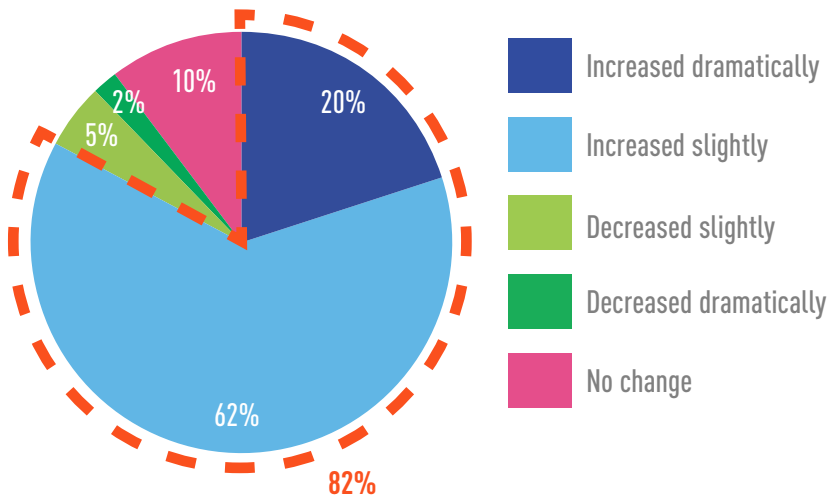


How have factors related to Covid-19 impacted *compliance* efforts in 2020?



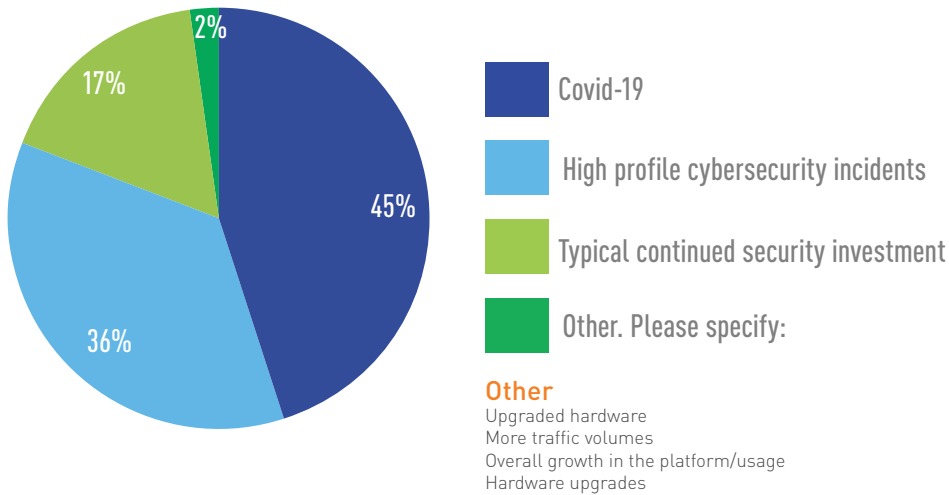
82% REPORT BIGGER SECURITY BUDGETS IN 2020, BUT ONLY SLIGHTLY FOR MOST

How has your company's overall security budget changed in the past year?



COVID-19 MOST COMMON CAUSE OF INCREASE IN SECURITY BUDGETS

What was the most significant drivers of security budget changes?
Choose the one answer that most closely applies.



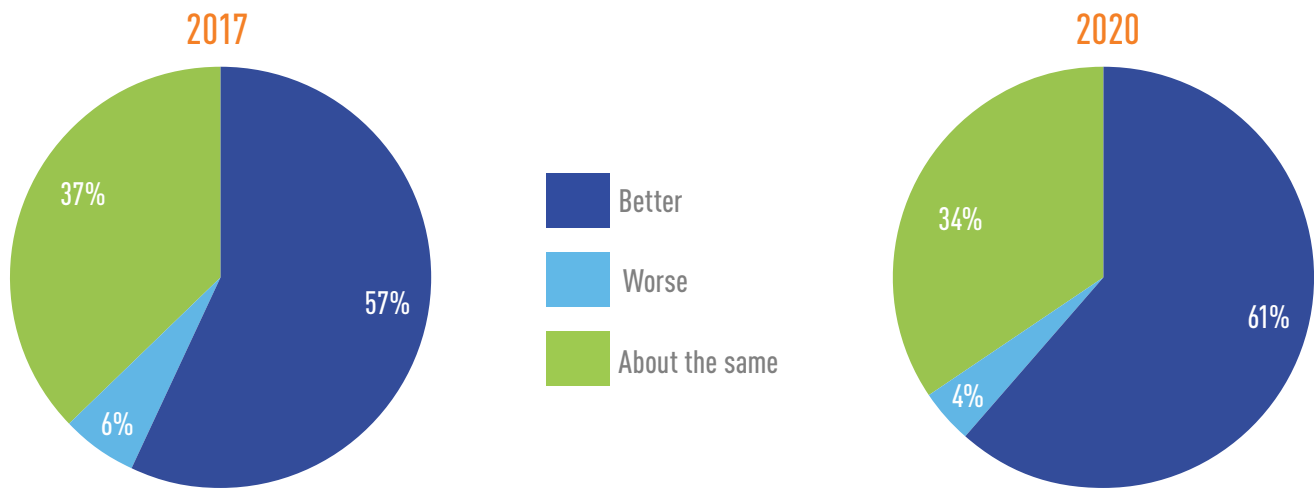
MOST SECURITY TEAMS AT RETAIL ORGANIZATIONS FEEL COMFORTABLE WITH THEIR INVESTMENTS, BUT WOULD PREFER MORE

How would you characterize your company's security investments and capabilities to detect and respond to a serious cybersecurity breach?



2020 SHOWS CONTINUED IMPROVEMENT IN ADDRESSING SECURITY BREACHES

Overall, how has your organization's ability to detect and respond to a security breach changed in the past 12 months?

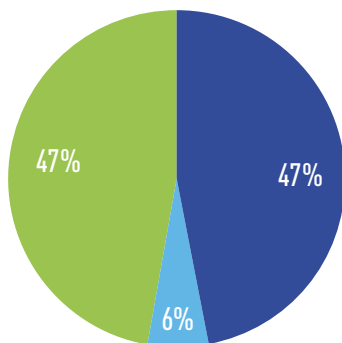


LARGE COMPANIES ARE MORE CONFIDENT IN THEIR IMPROVEMENTS

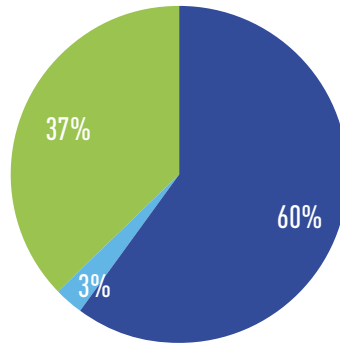
Overall, how has your organization's ability to detect and respond to a security breach changed in the past 12 months?

By Company Size (2020 Only)

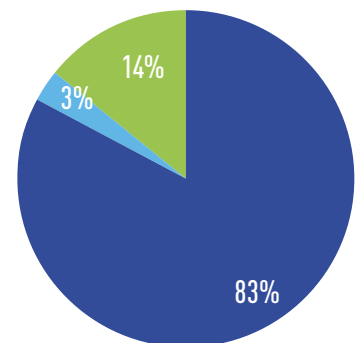
100-1000 EMPLOYEES



1000-5000 EMPLOYEES

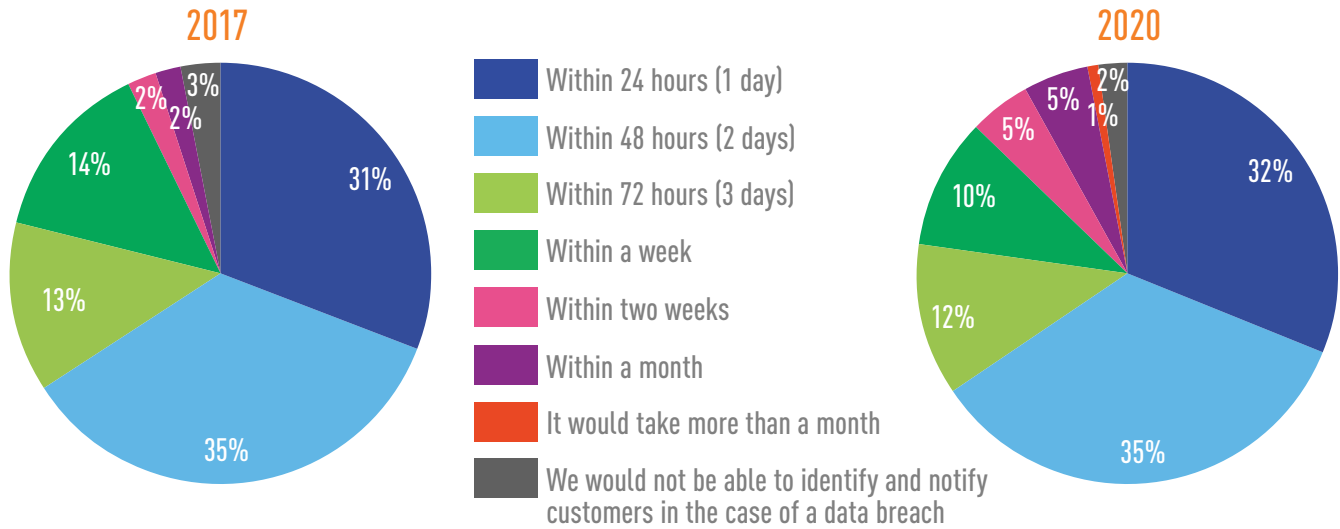


>5000 EMPLOYEES



ABILITY TO CONTACT CUSTOMERS OF A BREACH WITHIN 72 HOURS (GDPR REQUIREMENT) UNCHANGED SINCE 2017

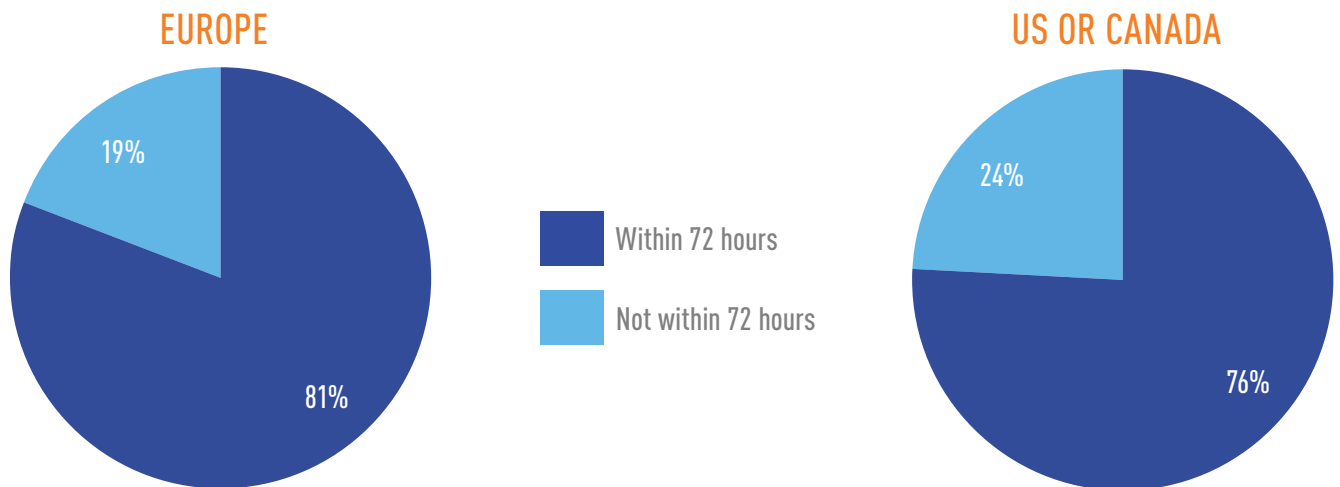
How long would it take your organization to notify customers of a security breach?



EUROPE ONLY SLIGHTLY MORE LIKELY TO MEET GDPR REQUIREMENT OF 72 HOURS

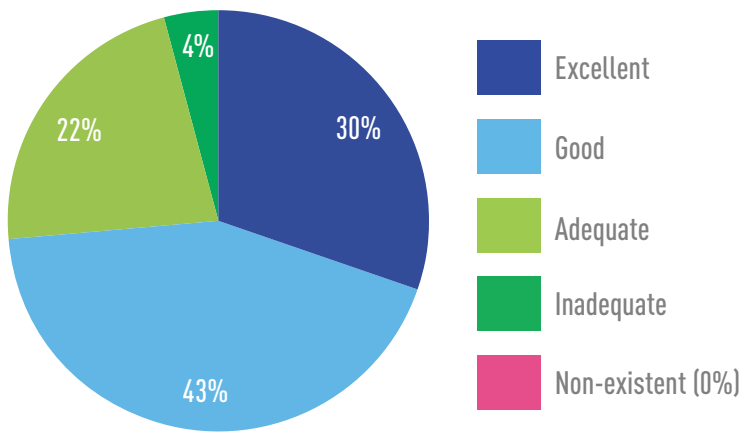
How long would it take your organization to notify customers of a security breach?

By Region (2020 only)



SLIGHT SHIFT IN ATTITUDES ABOUT AWARENESS OF LOCATION OF CUSTOMER DATA IN PAST YEARS

How would you characterize your company's capabilities for knowing *where* you store your customer data?



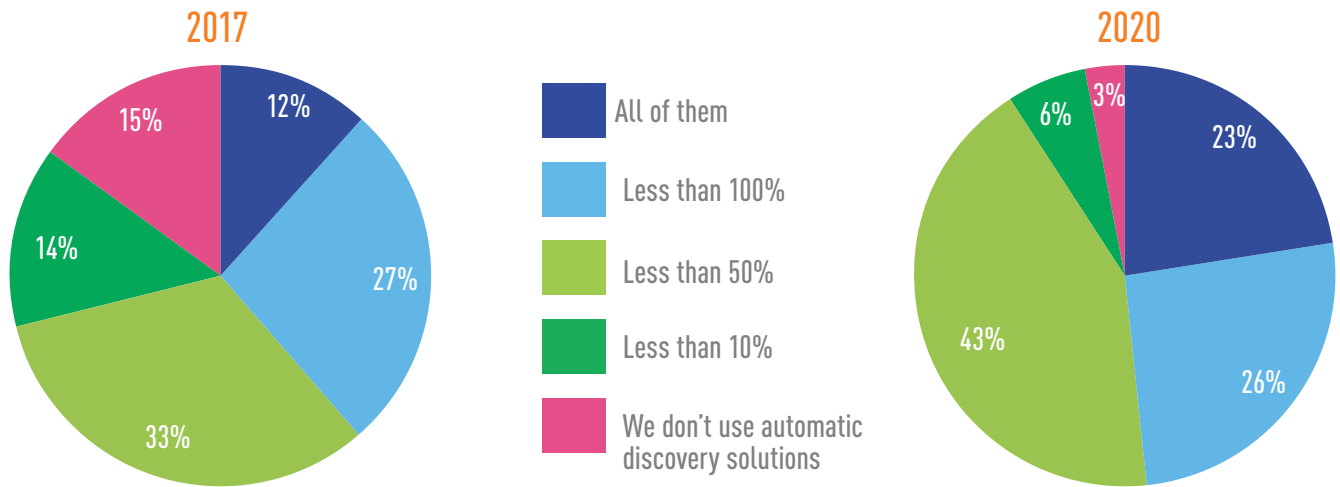
CONFIDENCE IN PROTECTING CUSTOMER DATA HAS INCREASED FOR RETAILERS

How would you characterize your company's capabilities for *protecting* your customer data (i.e. controls are enforced, systems are secured, etc.)?



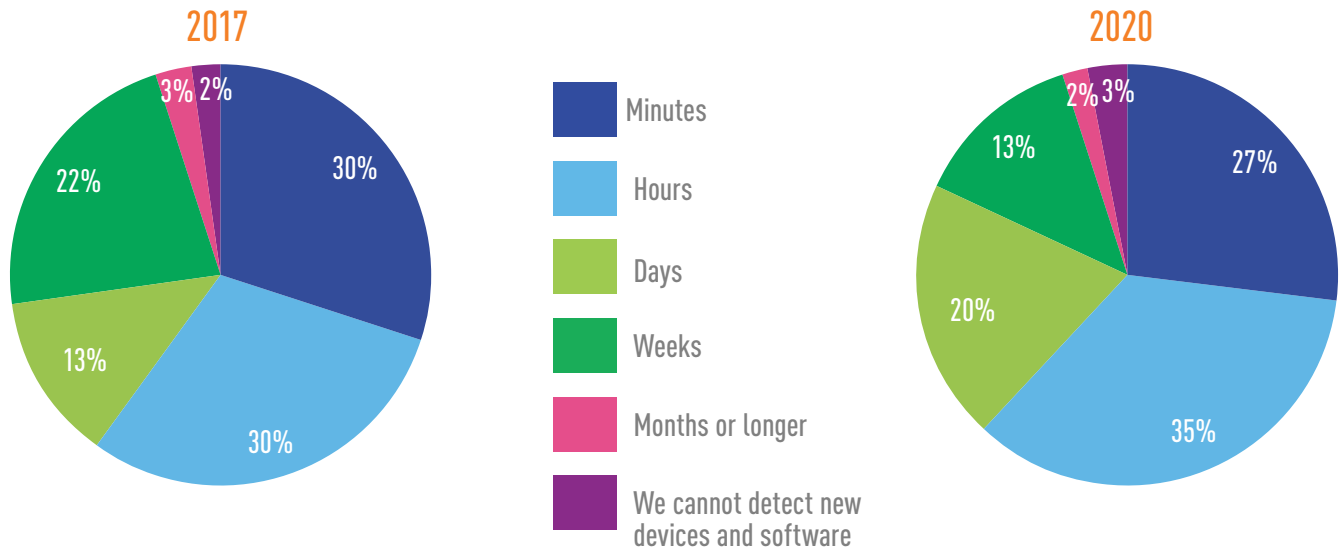
RETAILERS HAVE INCREASED AUTOMATIC DISCOVERY OF HARDWARE AND SOFTWARE ASSETS

Approximately what percentage of hardware and software assets on your network are discovered automatically?



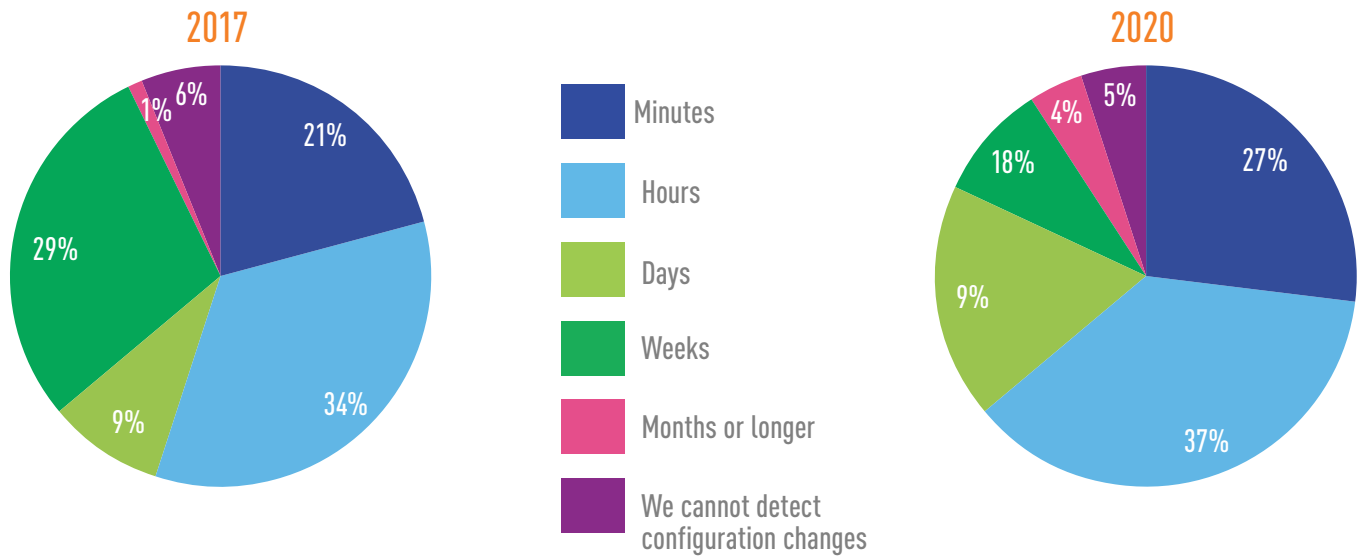
STILL, DETECTING NEW ASSETS TAKES HOURS OR LONGER FOR MOST ORGANIZATIONS

How long does it take to detect new hardware and software added to the organization's network?



DETECTION OF CONFIGURATION CHANGES IMPROVING COMPARED TO 2017

About how long does it take to detect configuration changes to hardware and software on your organization's network?



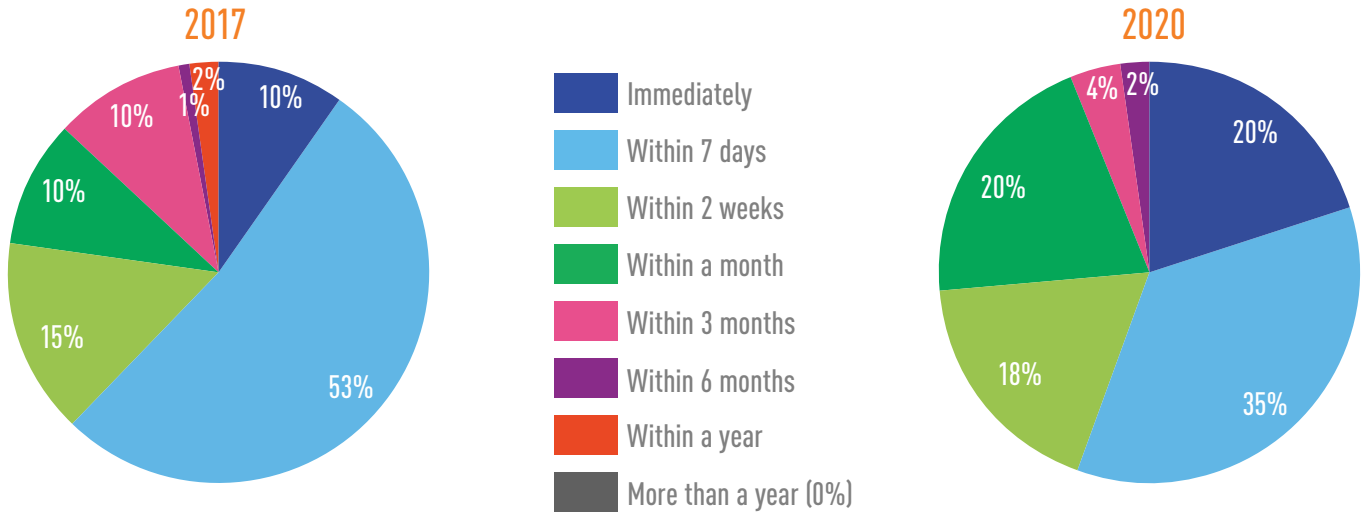
THE RATE OF ADDRESSING VULNERABILITIES HAS NOT CHANGED MUCH SINCE 2017

Are all vulnerabilities detected by scanning tools fixed or remediated promptly?



TWICE AS MANY ARE DEPLOYING SECURITY PATCHES IMMEDIATELY

In general, how long does it take to deploy a security patch in your environment?





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](#)