How Are Federal Agencies Responding to Recent Cyber-attacks?

March 2021

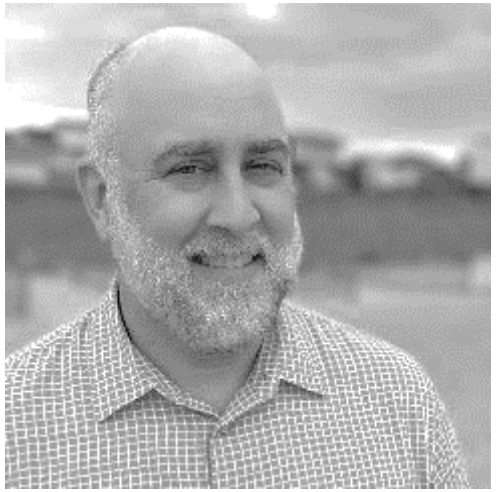
In partnership with:

ATARC

Market Connections®
Research you can act on.

Webinar Speakers

Aaron Heffron
Presenter
President
Market Connections



Tom Suder
Panel Moderator
Founder & President
ATARC

Webinar Panelists

John Alboum

Former CIO, USDA

Federal CTO & Principal Digital Strategist, *ServiceNow*

Chad Sheridan

Former CIO, USDA

Chief Innovation Officer, *NetImpact Strategies Inc.*

John Zangardi

Former CIO, DHS

President, *Redhorse Corp.*

About the Study

Methodology

Market Connections designed an online survey of 204 federal employees involved in IT security, operations and management at their agency.

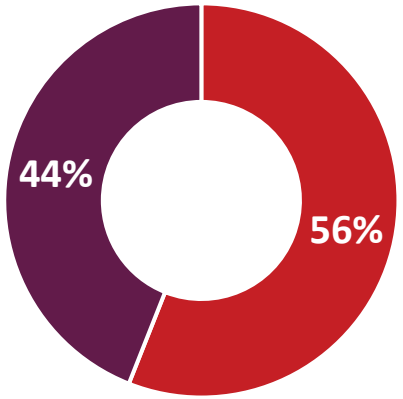
PRIMARY OBJECTIVES:

- Gauge the impact of recent federal cybersecurity breaches
- Analyze steps agencies have taken to mitigate cybersecurity threats
- Identify actions contractors can take to help agencies combat cybersecurity threats

Respondent Classifications

Respondents were screened to ensure they were involved in decision-making and had a high level of familiarity with IT security, operations and management in their agencies.

Agency Type



Job Title/Function

49% - IT staff
28% - Security team
11% - C-level
12% - Other

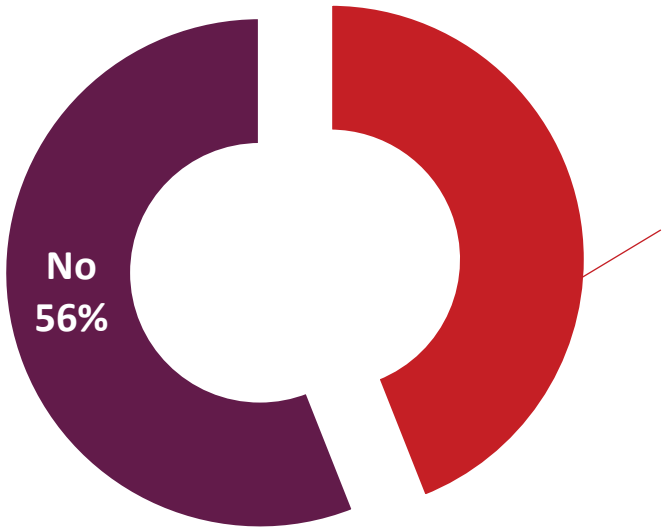
Involvement in Decisions Regarding IT Security and/or IT Operations and Management Solutions

Results

Impact of Recent Cybersecurity Breaches

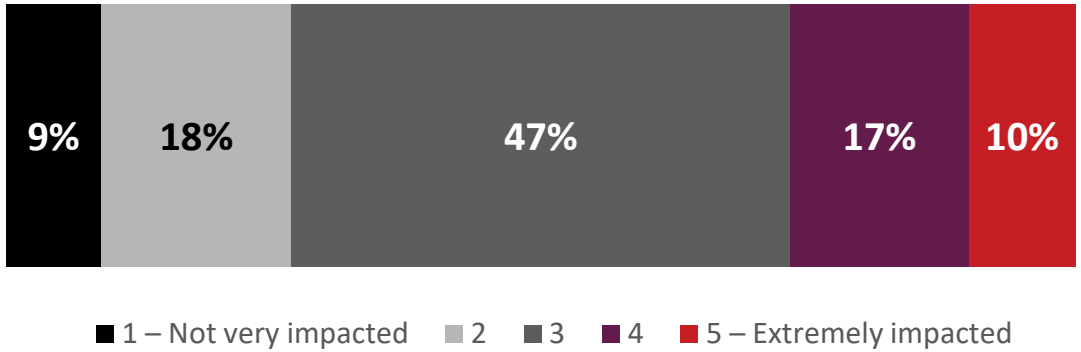
While nearly half were impacted by recent breaches, overall, the impact for most was not considered extremely significant.

Agency Impacted by Recent Cybersecurity Breaches



Yes
44%

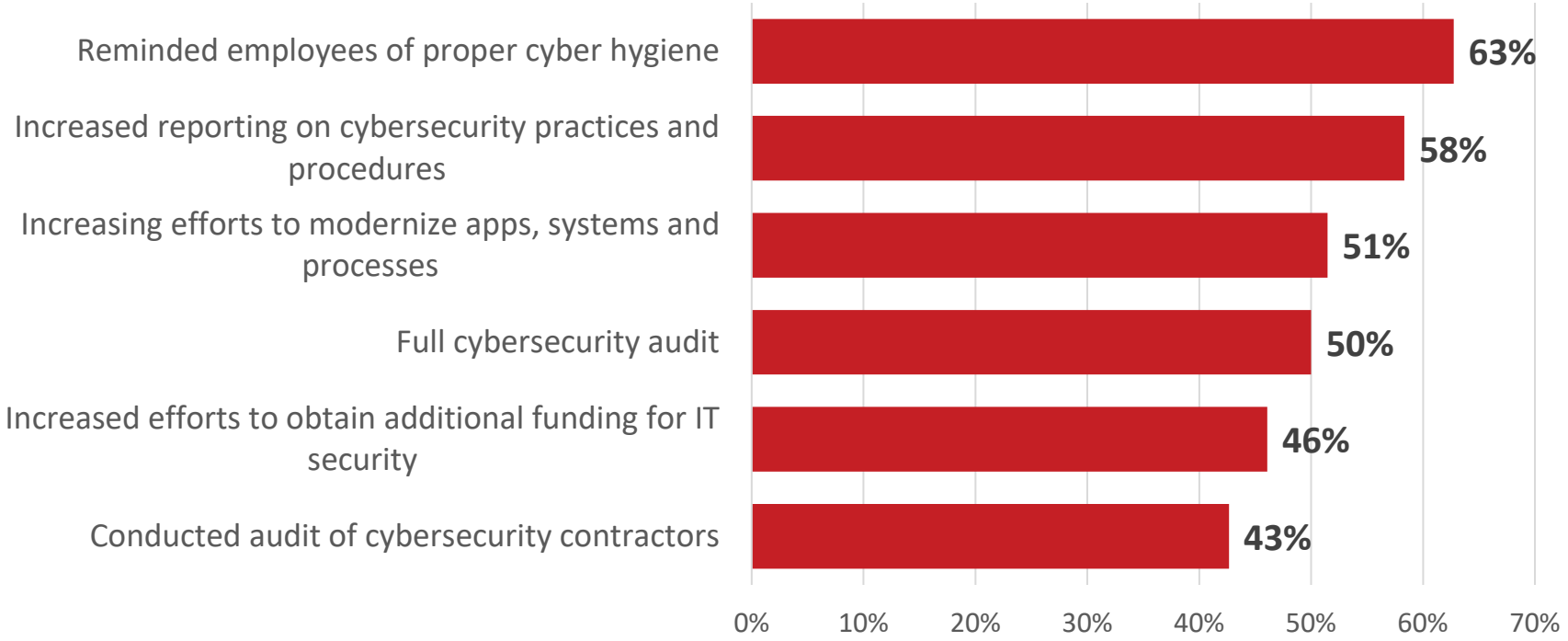
Level of Impact



Was your agency impacted by recent cybersecurity breaches?
[IF YES] How severely was your agency impacted by recent cybersecurity breaches?

Top Actions Taken in Response to Cybersecurity Breaches

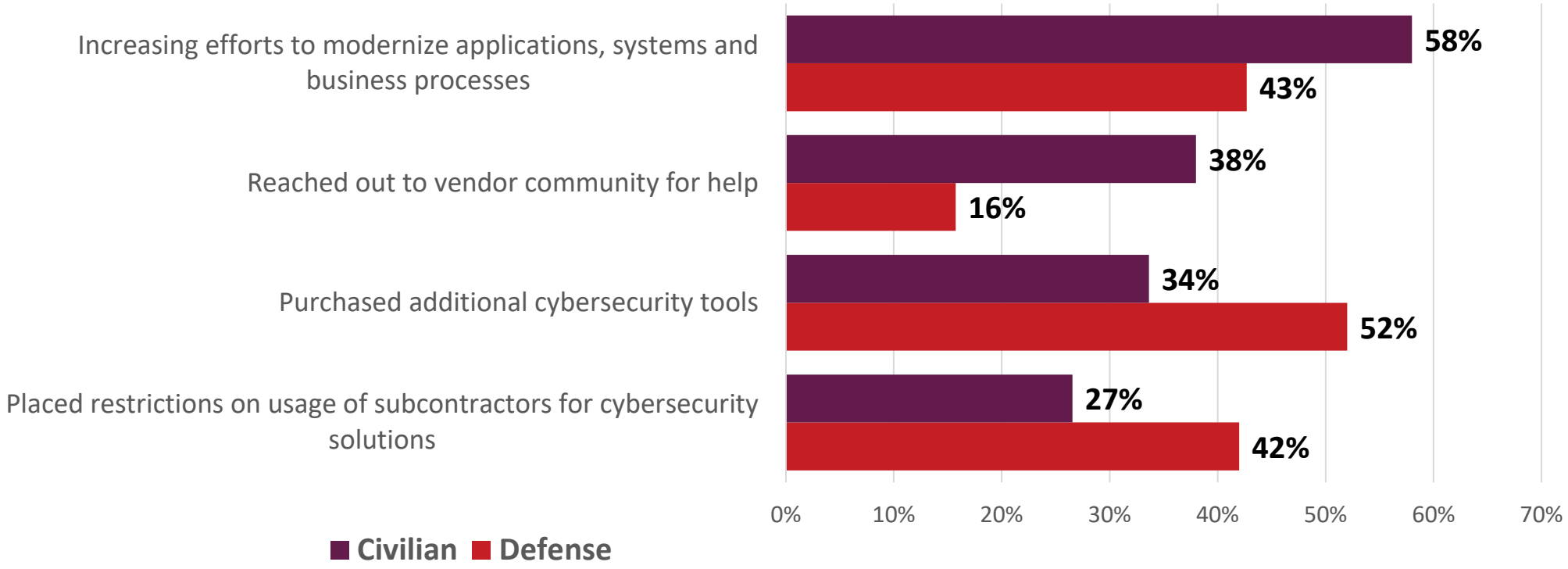
Recent cybersecurity breaches served as a reminder to revisit proper cyber hygiene, and increase/ improve auditing and reporting practices.



What actions, if any, has your agency taken or is planning to take in response to the recent cybersecurity breaches?

Response Actions Taken by Agency Type

While civilian agencies are more likely to have reached out to the vendor community and increased efforts to modernize, defense/intel agencies were more likely to place restrictions on subcontractors and purchased additional tools.



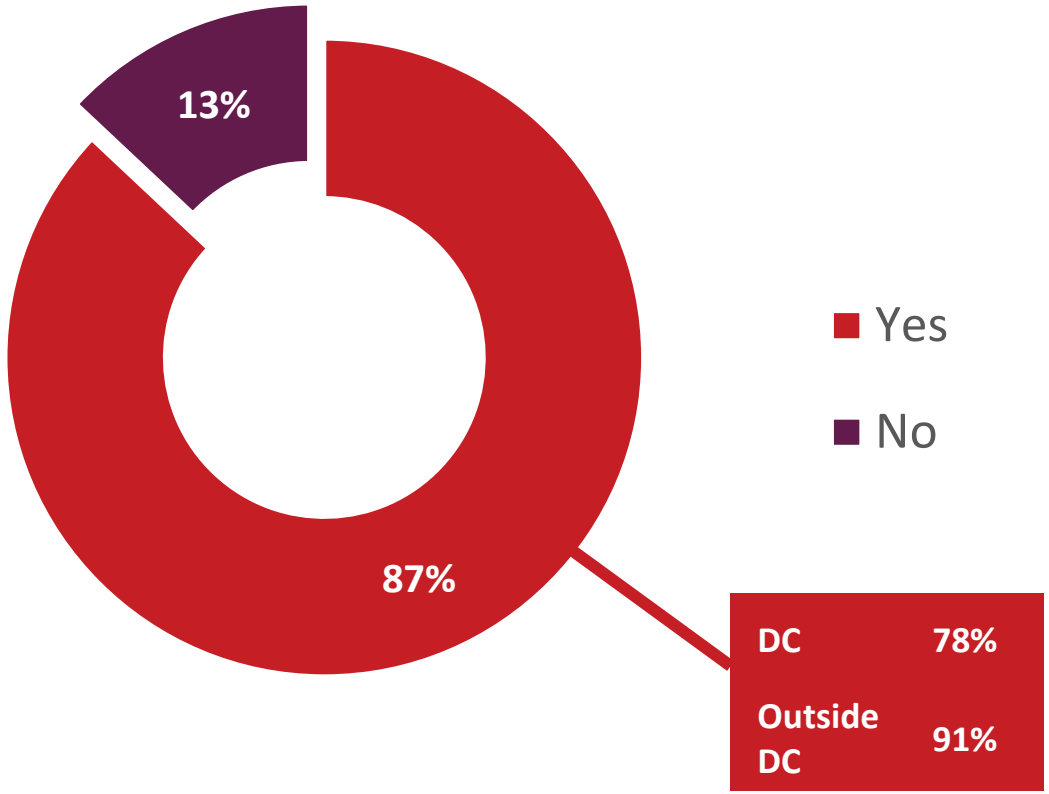
What actions, if any, has your agency taken or is planning to take in response to the recent cybersecurity breaches?

Actions Vendors Have Taken

Vendors have been proactive about making recommendations and suggesting new solutions.

What actions have your vendors who provide cybersecurity systems and solutions taken in response to the recent cybersecurity breaches?

Vendors Proactively Providing Support



> They are involved in all aspects of our program. The CISO office had increased contractors support. Agency provided additional funding.
>
> NASA

> Our vendors immediately began a cyber review of their systems and notified us of any issues related to the breach.
>
> CFPB

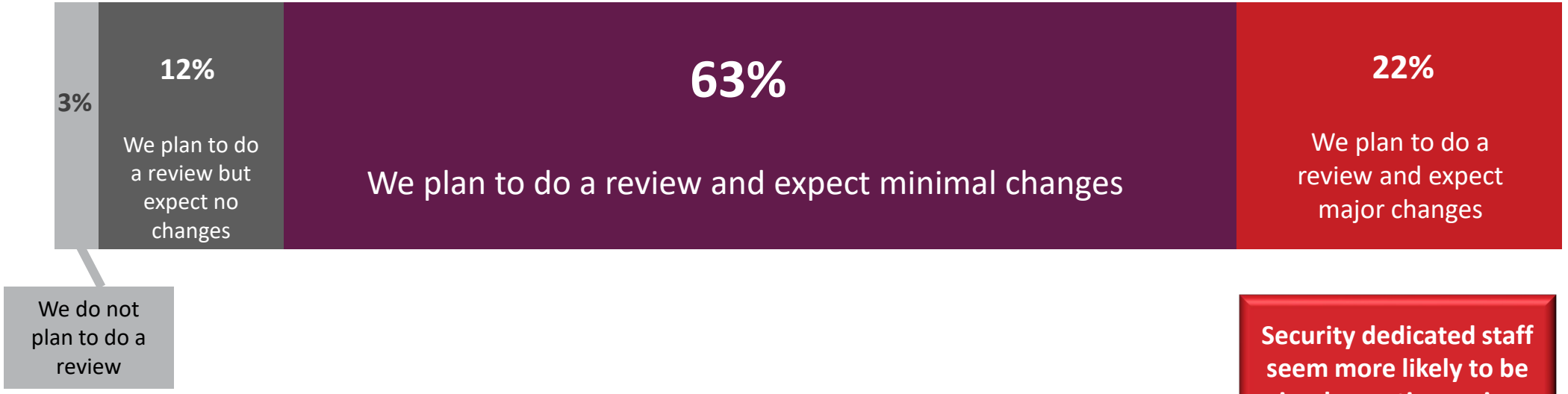
> They do the status quo and that's it. We need to continuously enforce cybersecurity standards and controls to adhere and comply to.
>
> DEPT OF TRANSPORTATION

> Vendors need to be more proactive in dealing with issues like this one.
>
> AIR FORCE

Do you believe your vendors have been adequately proactive in supporting you and your agency in response to the recent cybersecurity breaches?
What did your vendors [do/not do] well in proactively supporting you and your agency in response to the recent cybersecurity breaches?

Plans to Review Cybersecurity Measures

While nearly all plan to do a review, overall, minimal or no changes are expected.

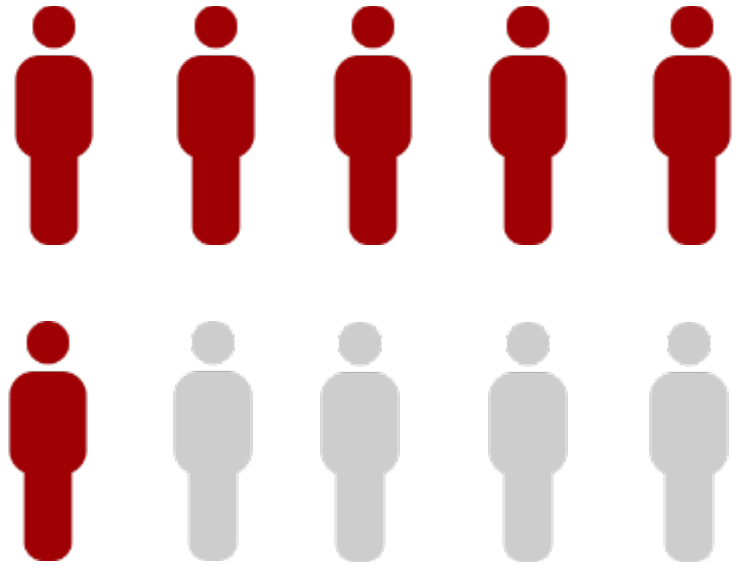


Security dedicated staff seem more likely to be implementing major changes

What are your agency's plans to review its cybersecurity measures in response to the recent cybersecurity breaches?

Classification of Recent Cybersecurity Breaches

6 out of 10 Classified Breaches Similar to Those in Past



> Mode of operation and hacking is very similar to previous breaches, it's just that the scale on which it's done is huge in recent ones.
>
> ARMY

> If you pay close attention, you would know they are all EXACTLY SIMILAR in their modus operandi.
>
> HUD

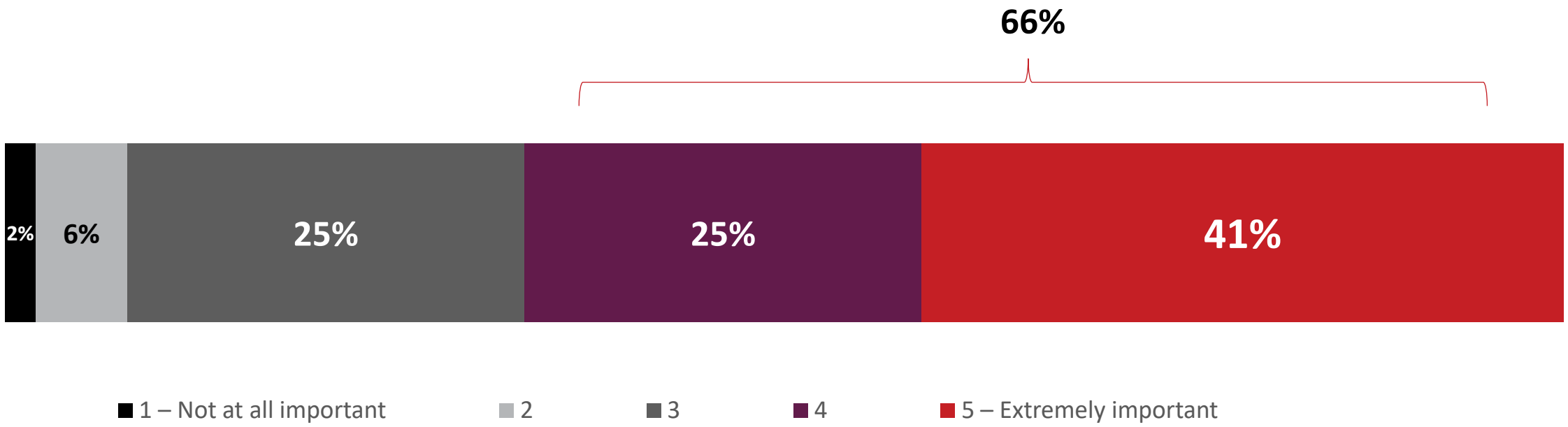
> These cybersecurity breaches were different because of the level of infiltration into systems and accounts, not ever seen before.
>
> DEPT OF JUSTICE

> They are always sightly different. the enemy is always adjusting to probe our defenses.
>
> DEPT OF TRANSPORTATION

Would you classify the recent cybersecurity breaches as unique and different than others in the past, or were they similar to breaches in the past?
Why would you classify the recent cybersecurity breaches as [PIPE IN]?

Importance of Citizens' Perceptions of Cybersecurity

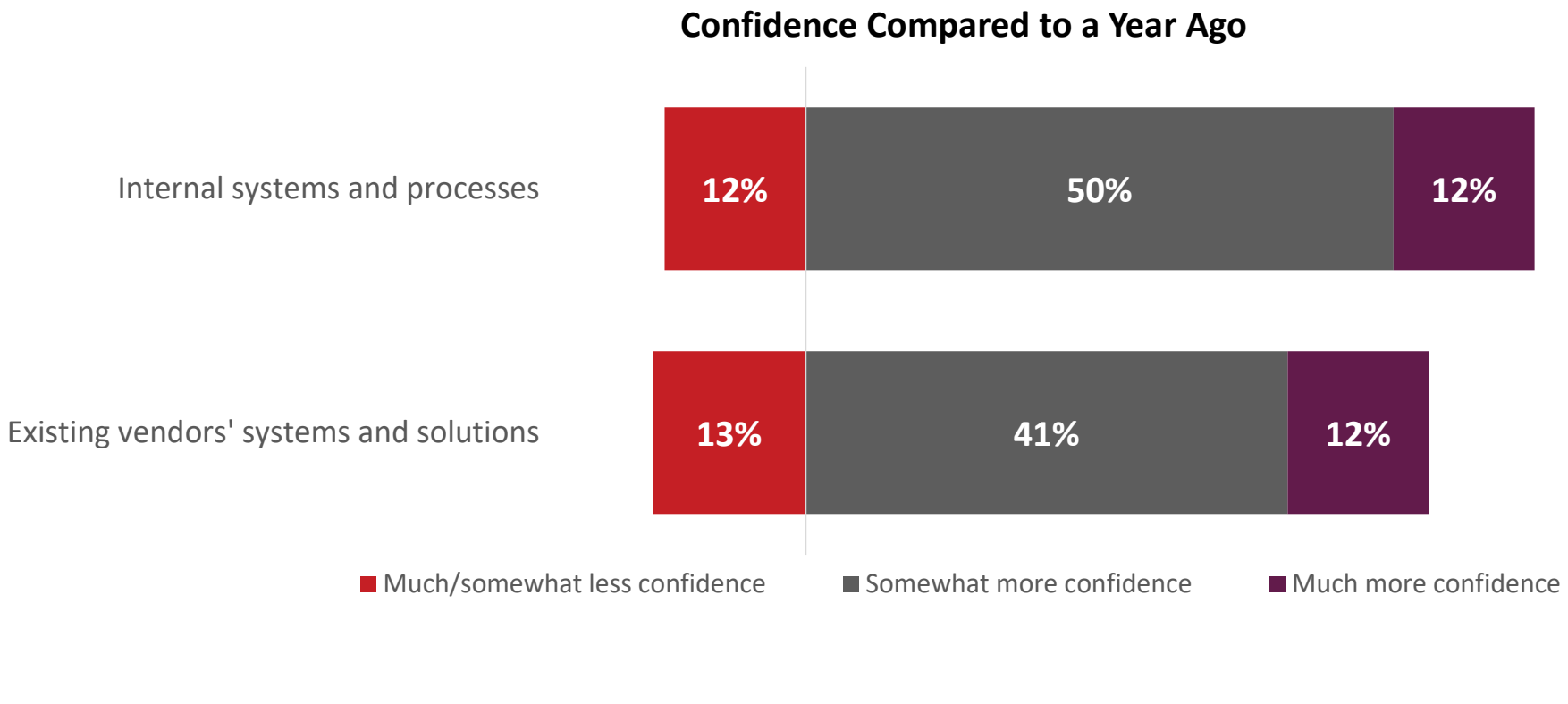
Most think citizens' perceptions of agencies' cybersecurity is very important.



How important are the citizens' perceptions of cybersecurity to your agency?

Internal and External Confidence in Thwarting Cybersecurity Attacks

Despite the breach, respondents were generally more confident in their systems than before.



Much/somewhat less confidence: Internal
DC: 24% Outside DC: 8%

Much/somewhat less confidence: Vendors
DC: 26% Outside DC: 9%

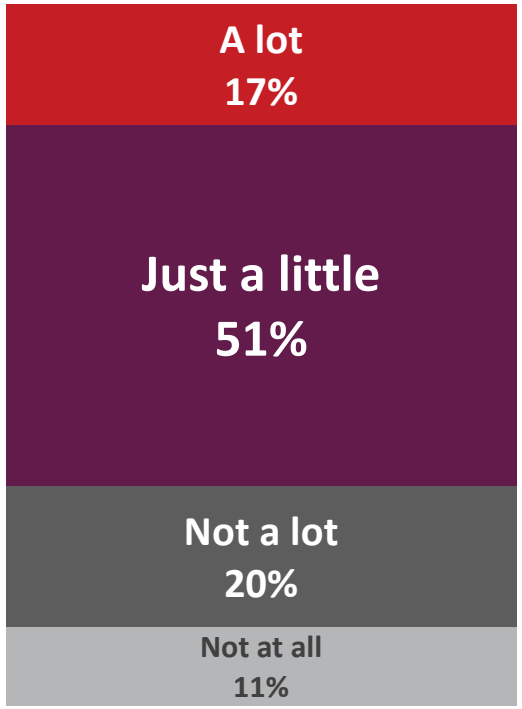
Security dedicated staff have gained confidence in vendor systems

Compared to a year ago, how much confidence do you have in your current internal systems and processes to thwart cybersecurity attacks?
Compared to a year ago, how much confidence do you have in the existing vendors' systems and solutions to support you in thwarting cybersecurity attacks?

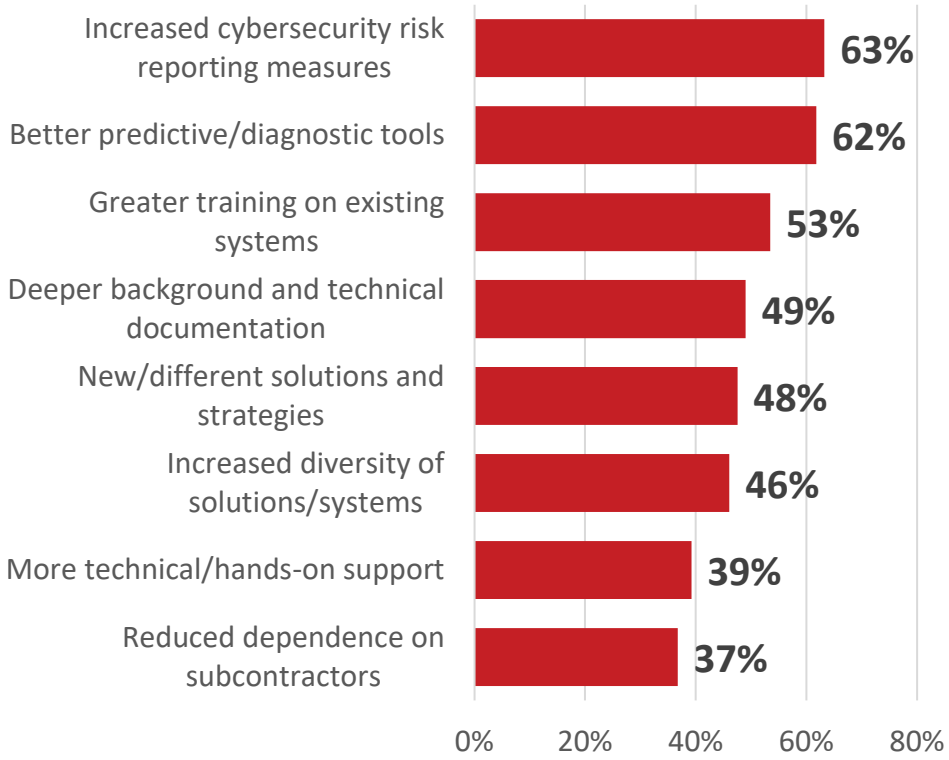
Relationship With and Needs From Vendors

Overall, relationships between vendors and agencies have not changed much. Agencies will be looking for more reporting measures and better predictive/diagnostic tools.

Extent to Which Breaches Changed Way Working With Vendors



Needs From Vendors



To what extent have the recent cybersecurity breaches changed the way you are working with your vendors that provide cybersecurity systems and solutions?
What do you need from the vendor community going forward to continue to combat cybersecurity breaches?

Key Takeaways

Key Takeaways

It’s a PROCESS, requires PROPER PROCEDURES and PROACTIVE PARTNERSHIPS .

- **The PROCESS has only begun. New information and breaches will likely come to light. Don’t be afraid to embrace the process.**
- **Vendors need to provide appropriate tools for monitoring, but also need straightforward, non-technical marketing documents detailing how they are adhering to PROPER PROCEDURES. These documents should demonstrate best practices and provide advice.**
- **PROACTIVE PARTNERS will step forward with new solutions for reporting and diagnostics as well as ways that agencies can reassure citizens and lawmakers.**

Panel Discussion

Panel Discussion

Tom Suder
Panel Moderator
Founder & President
ATARC

John Alboum
Former CIO, USDA
Federal CTO & Principal Digital Strategist, *ServiceNow*

Chad Sheridan
Former CIO, USDA
Chief Innovation Officer, *NetImpact Strategies Inc.*

John Zangardi
Former CIO, DHS
President, *Redhorse Corp.*

Save the Date

Content Marketing Review: FED & SLED

Date: Thursday, May 20, 2021
Location: Online

Other Market Connections Studies & Resources

- 2020 Federal Media & Marketing Study
  https://www.marketconnectionsinc.com/fmms2020study/
- Webinar: The Continued Effects of COVID-19 on the Federal Contracting Industry and Your Customer
  https://www.marketconnectionsinc.com/the-continued-effects-of-covid-19-on-govcon-and-your-federal-customer/
- 2020 FIT (Federal IT) Personas Study
  https://www.marketconnectionsinc.com/fit-federal-it-persona-study-2020-a-deeper-look-into-your-government-customer/
- Market Connections Federal Central
  www.marketconnectionsinc.com/fedcentral/

ATARC Events and Resources

- Data Management for Hybrid and Multi-Cloud (March 4, 1:30)
  https://atarc.org/event/data-hybrid-multi-cloud/
- Cyber Compliance Boosted by Automation (March 9, 1:30)
  https://atarc.org/event/automated-cyber-compliance/
- ATARC 2021 Zero-Trust Virtual Summit (March 11, 1:30)
  https://atarc.org/event/zero-trust-2021/

- Learn more about ATARC's Learning Groups:
  https://atarc.org/working-groups/
  Contact Kiersten Patton: kpatton@atarc.org

Contact Information

Aaron Heffron, *President*

703.966.1706
AaronH@marketconnectionsinc.com

Tom Suder, *Founder & President*

703.786.6309
Tsuder@atarc.org

ATARC

Market Connections®
Research you can act on.