TITANIA
Assured Accuracy

Research Study

The impact of exploitable misconfigurations on the security of agencies' networks and current approaches to mitigating risks in the U.S. Federal Government

Research conducted by:

COLEMAN PARKES RESEARCH

Contents

Introduction

Sophisticated cyber threats are headline news. As are attempts to defeat them, with threat intelligence, hunting, and detection and response programs rightly holding the spotlight on the cyber stage for a long time.

But increasingly, exploitable vulnerabilities, and how to prevent them, are back on the agenda. Particularly as recent attacks on critical national infrastructure organizations have utilized arguably less sophisticated tactics to exploit network vulnerabilities. Moreover, high profile security breaches that have used misconfigured routers and switches as a way into networks, are not as rare as they ought to be. Indeed, the NSA, CISA and FBI recently issued a joint Cybersecurity Advisory pointed to attackers altering network device configurations to enable and scale their attacks.

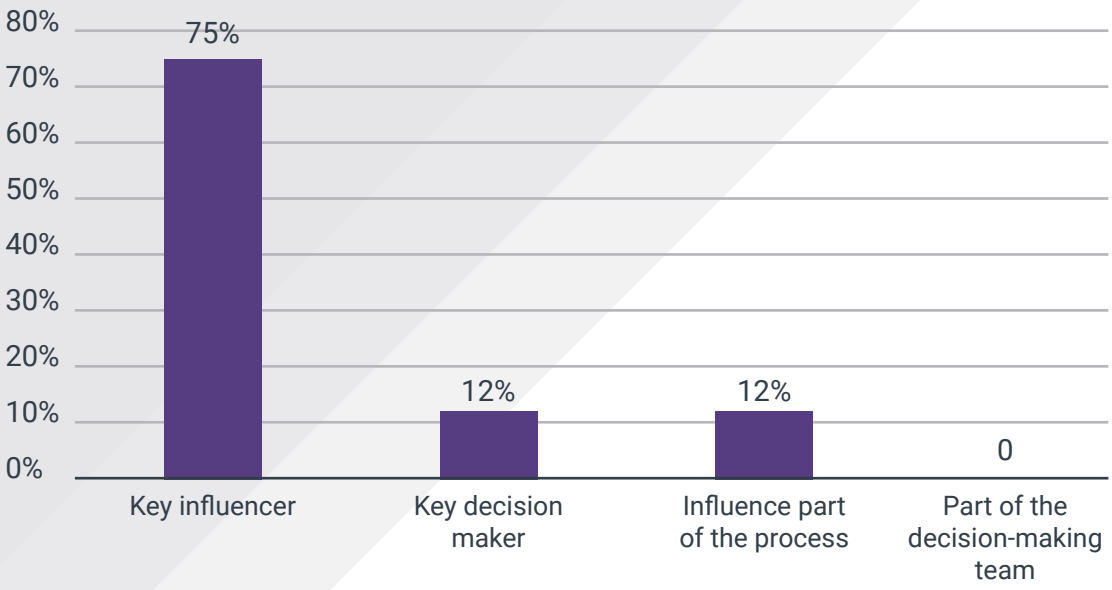
Ultimately, a truly determined attacker will try a combination of approaches to access a network until they gain entry—typically by targeting a known vulnerability or misconfiguration. It's why the White House released a federal strategy to drive US government agencies towards adopting a zero trust approach to cybersecurity, where hardening networks from the inside-out makes it as difficult as possible for intruders to gain entry and progress towards their goal by inhibiting lateral movement. And why Attack Surface Management (ASM) best practices encourage organizations to show continuous vigilance, and approach security tasks like asset discovery, identification, inventory and assessment from an attacker's perspective.

This kind of proactive security is key to protecting critical networks from preventable attacks. It acknowledges that security within the network boundary is as important as the security on devices forming the perimeter.

Networks are constantly changing, as often as on a daily basis. Configuration drift can, and does, go undetected between configuration audits. So Titania wanted to understand more about how the U.S. Federal Government is currently managing the critical risks associated with misconfigured network devices – namely firewalls, switches and routers. We commissioned independent B2B research specialists, Coleman Parkes, to investigate by surveying senior cybersecurity decision-makers across the US federal government, as well as other US critical national infrastructure sectors (military, oil & gas, telecoms, and financial services), for comparison purposes.

The survey asked how organizations currently detect and mitigate vulnerabilities in the specified part of the network. And how confident they are that devices maintain a secure configuration at all times.

Networking Role



Executive summary:

Highlights from federal government respondents

Based on the insights provided by the CIOs, Heads of Networks, Network Architects, and other experts, who participated in the survey, the report highlights four key findings that need to be addressed in order to protect federal government from preventable attacks, in line with best practices.

The four key findings (see conclusion) were consistent for the other sectors surveyed – it was the size of the network which differed, with the average number of firewalls, switches and routers that protect the federal government respondents needed to secure sitting at just over 1000 devices. An average of 160 more than the next highest sector (banking and financial services).

Indeed, the 'size of the network' figures for federal government were akin to those in very large organizations, and perhaps unsurprisingly, government respondents reported the joint highest IT budgets. Yet the proportion of annual IT budget allocated to network configuration risk management in federal government was consistent with the average across all sectors at just 3.2%.

The federal government's task of defending such large networks against preventable attacks is no easy feat, within its budget constraints. Particularly when we consider that remediating devices for misconfigurations and other exploitable vulnerabilities is just one in a long list of best practices that Network Operations Centers are charged with daily.

Unlike software vulnerabilities which can be "patched away", misconfiguration risks – which often pose a more significant risk to security – cannot. In these cases, network security teams first need visibility of misconfigurations before they can assess the risk they pose to the network. They then need to prioritize fixes based on risk to inform remediation workflows. As networks grow and become more complex, these tasks become more challenging, but remain the basis of good cyber hygiene.

Interestingly, the survey found federal government agencies surveyed were more likely to describe their level of maturity to network security as higher, with 65% reporting that they had full measurement of KPIs, against an average of 48% in other sectors. Yet the lowest percentage of respondents (18%, compared to 34%+ in other sectors) that were 'very confident' that other players in their organization's supply chains take a rigorous and robust approach to network configuration security. The federal government also made up the highest percentage (71%) of respondents that reported relying on suppliers' external accreditations from CMMC, DISA, NIST, FISMA and ISO to gain assurances regarding supply chain risk management.

It's also important to note another key finding from this survey: federal government respondents were the only sector representatives to say that they exclusively assessed the configurations of their firewalls. Switches and routers were not included in their network checks. The federal government was also more likely to review and validate its network device configurations annually, rather than quarterly, which was the popular answer for the other sectors. But, according to the respondents, these practices were sufficient to meet with their security and compliance requirements.

The next chapter examines the wider survey findings in more detail, providing graphical context that shows despite the fact the federal government is unique in many ways with its own set of regulations, budget requirements and pace of change – it has the same challenges and therefore priorities as other sectors when it comes to securing the network. Namely:

1. Validating network configurations is a top three priority for all organizations,

2. The shift from ad-hoc to continuous assessment of configuration risks is strategically important, and the

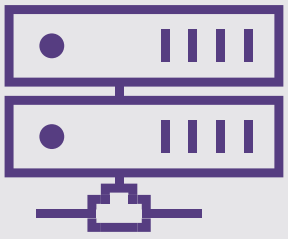
3. Inability to prioritize remediation based on risk is the biggest challenge.

Read on to find out what this means in practice…

Self-reflection:

Respondents are confident that their current networks are secure

During the survey, each respondent was asked a series of questions on the topic of network security to ascertain how their organizations are currently managing vulnerabilities. All respondents are network security and/or compliance decision-makers, knowledgeable about the fundamental role that correctly configured firewalls, switches and routers play in protecting their networks. They understand that these network devices are not only more complex than endpoints, but also pose more risk to the organization if exposed and exploited. And they are also familiar with the methods their organization uses to defend their firewalls, switches and routers from preventable attacks.

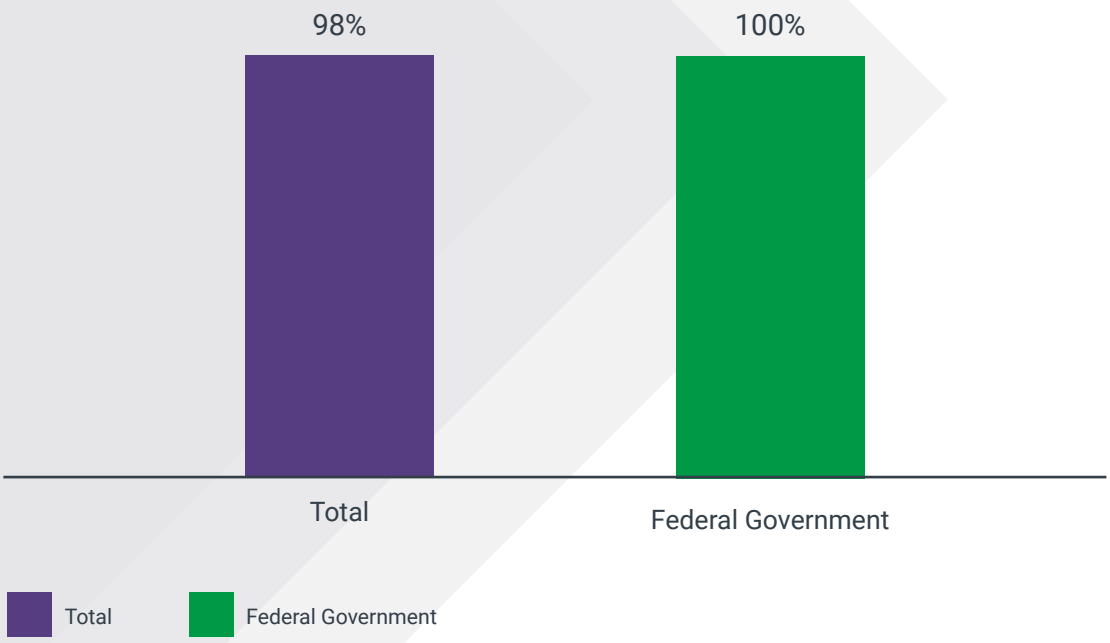


The survey started with questions regarding the organization's approach to network security and compliance. Here are the results from the federal government respondents, alongside comparison averages from the total set of respondents.

Federal government organizations report they are meeting security and compliance requirements

Every respondent from the federal government sector was confident that they are meeting their corporate security and external compliance requirements. This is an important finding when more than 88% of federal government respondents agreed that their organization relies on compliance to deliver security (compared to the 75% average across all sectors).

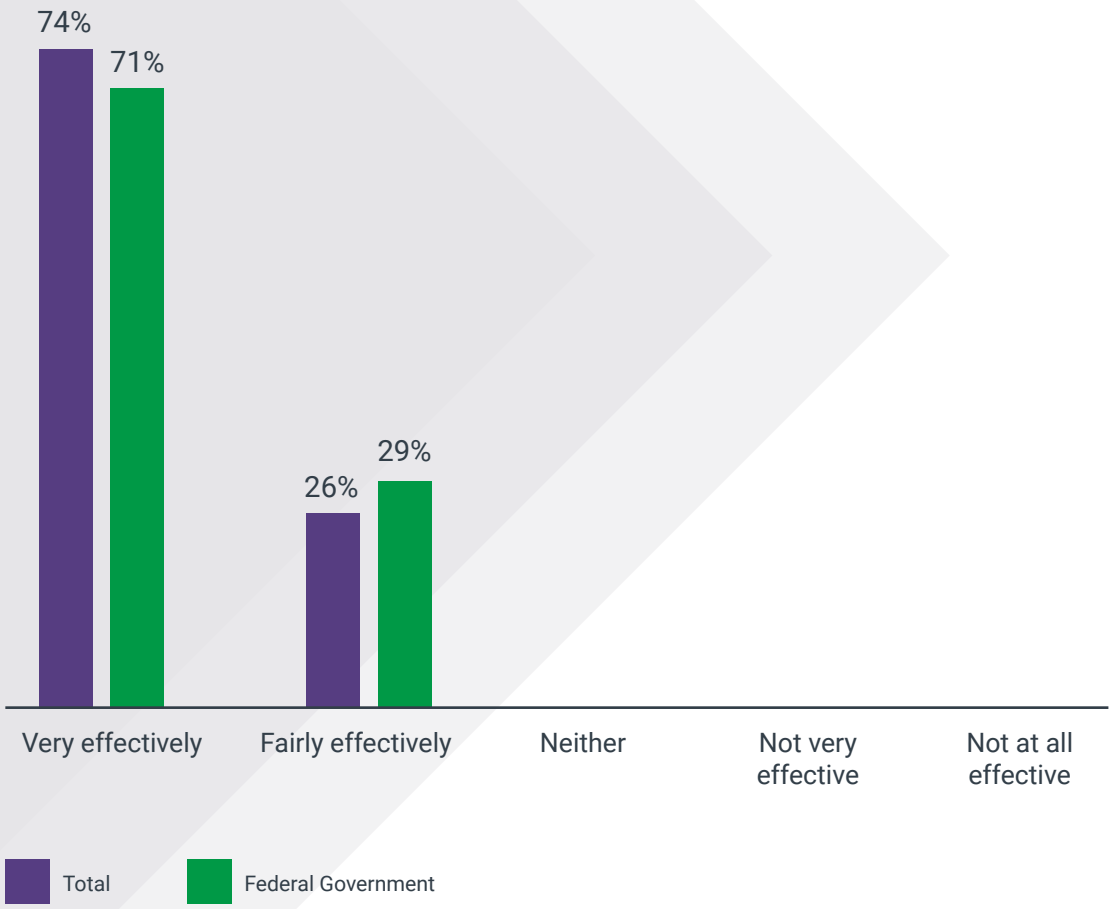
Q1. Are you meeting your corporate security and external compliance requirements? (Yes responses)



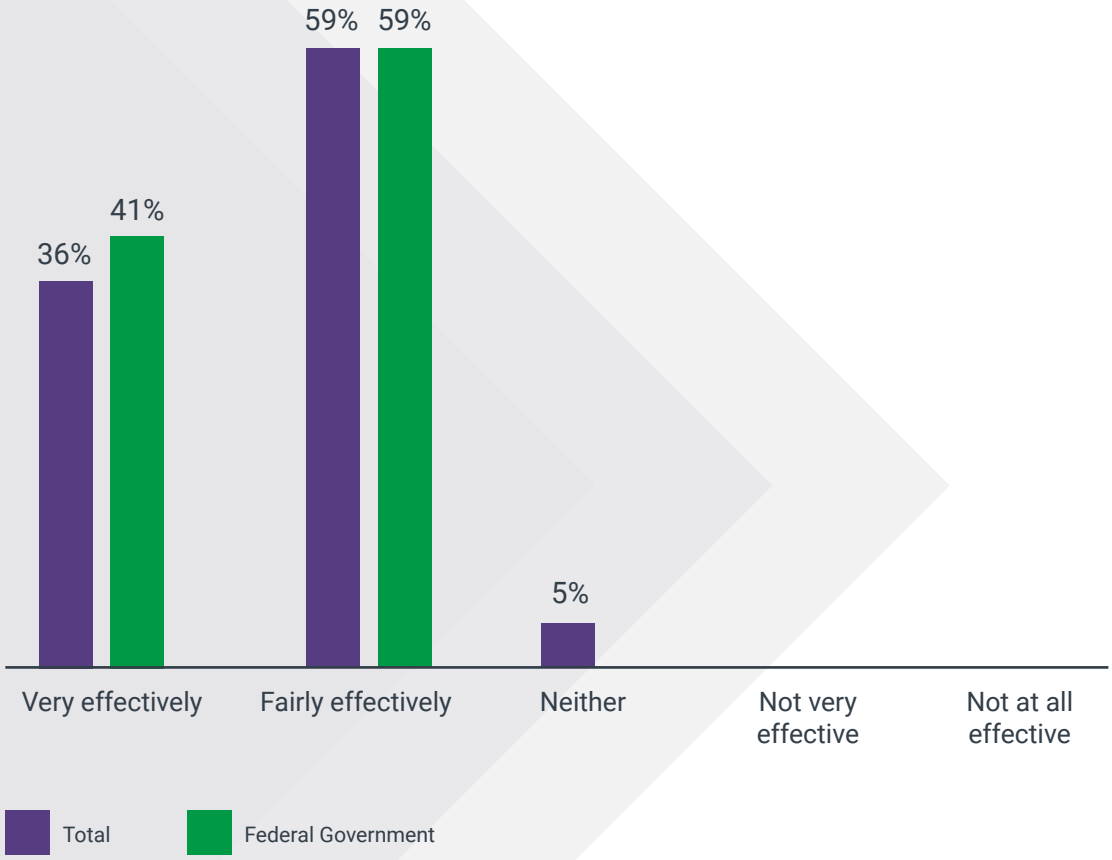
Self-reflection: (contd)

Just under three-quarters of federal government respondents said that their network security tools meant they could categorize and prioritize compliance risks very effectively. All of the rest said they could do so fairly effectively. This was largely consistent with the averages for the total dataset.

Q2. To what extent do your network security tools allow you to effectively categorize and prioritize identified security and compliance risks?



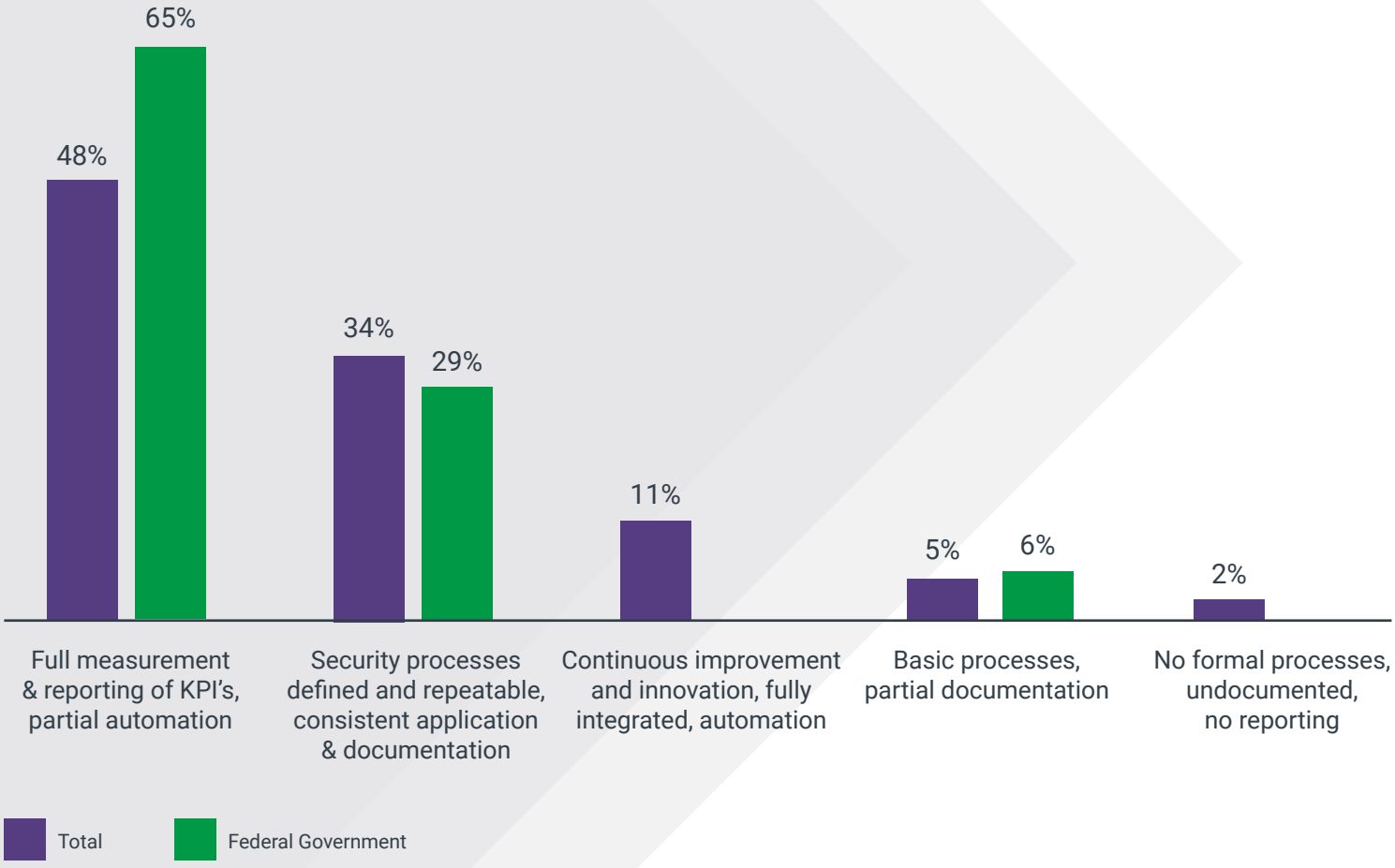
Compliance risk



Self-reflection: (contd)

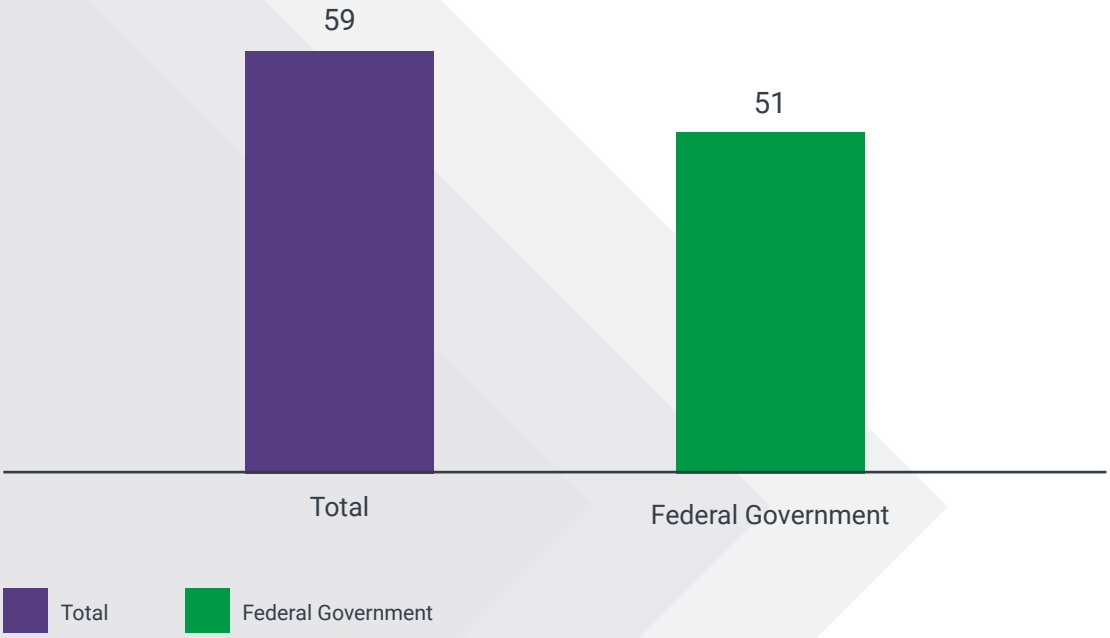
The survey revealed higher levels of confidence when government respondents were asked to think about the processes and infrastructure their organization had in place for managing the security of firewalls, switches and routers across a network. Most assessed their organization's current approach as mature.

Q3. Typically, how would you assess your current level of maturity when it comes to the processes and infrastructure your organization has in place for managing the security of firewalls, switches and routers across your networks?



Nearly two thirds (65%) said that they had full measurement and reporting with some automation whilst a further 29% said that their security processes were at least documented and repeatable. The remaining 6% had basic processes, so no federal organization had 'no formal processes' in place.

Q4. How many misconfigurations in total have been identified in (1) the past 12 months



Validating network configurations is a top three federal government priority

Validating network configurations is seen as a top three consideration for 88% of federal government network security teams, compared to the cross-sector average of 92%. Every single respondent from this sector also confirmed that validating network configuration security was a part of their overall risk management strategy.

The processes that federal organizations have in place means that they are picking up misconfigurations—an average of 51 in the last year, just shy of the total sector average of 59. Of the 51, respondents reported that four percent were "critical" misconfigurations that could have led to a serious breach of security.

Respondents revealed that they are aware of the cost that misconfigurations are causing their organization; a cost that is largely consistent with the total cross-sector average. The federal government also estimates that around 13% of resources from various teams are used for network configuration risk management activities, which is again consistent with findings from the other sectors.

Deep-dive:

Understanding current configuration assessment processes

Networks can change on a daily basis. It's why many risk management and security control frameworks/programs – such as the DHS's Continuous Diagnostics and Mitigation (CDM) program and the DoD's Comply-to-Connect (C2C) program – recommend or require continuous monitoring of all network devices. This is to ensure a regular cadence of assessment to detect and mitigate vulnerabilities (both software and misconfigurations), before they can be exploited. As left undetected, and therefore unmitigated, vulnerabilities could compromise the confidentiality, integrity, and availability of critical data and/or applications. And such compromise can cause the federal government significant operational and mission issues.

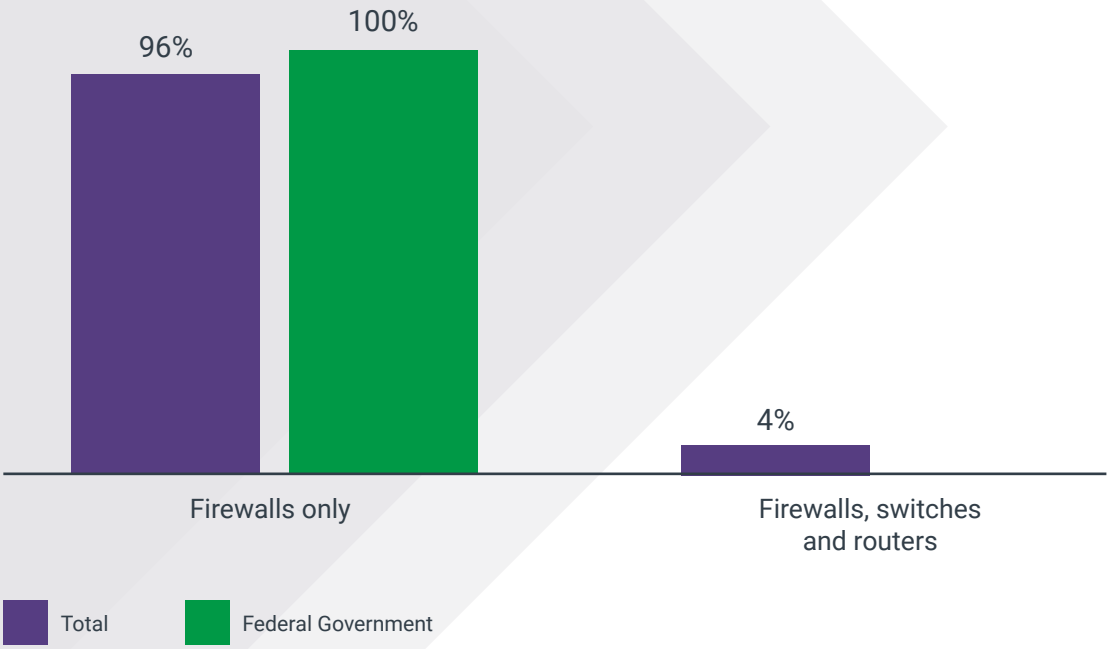
The next set of questions asked respondents to share information about how and when they assess networks for vulnerabilities and validate that configurations are secure.

Q5. How often do you assess the network configuration settings of firewalls, switches and routers within your organization?

Annual configuration assessments are typical for the majority of federal government organizations

Most (59%) assessed the configuration of network devices on an annual basis. Only 12% assessed them more frequently than once a month.

Q6. When scanning, do you assess:



All federal government organizations only assess their firewalls

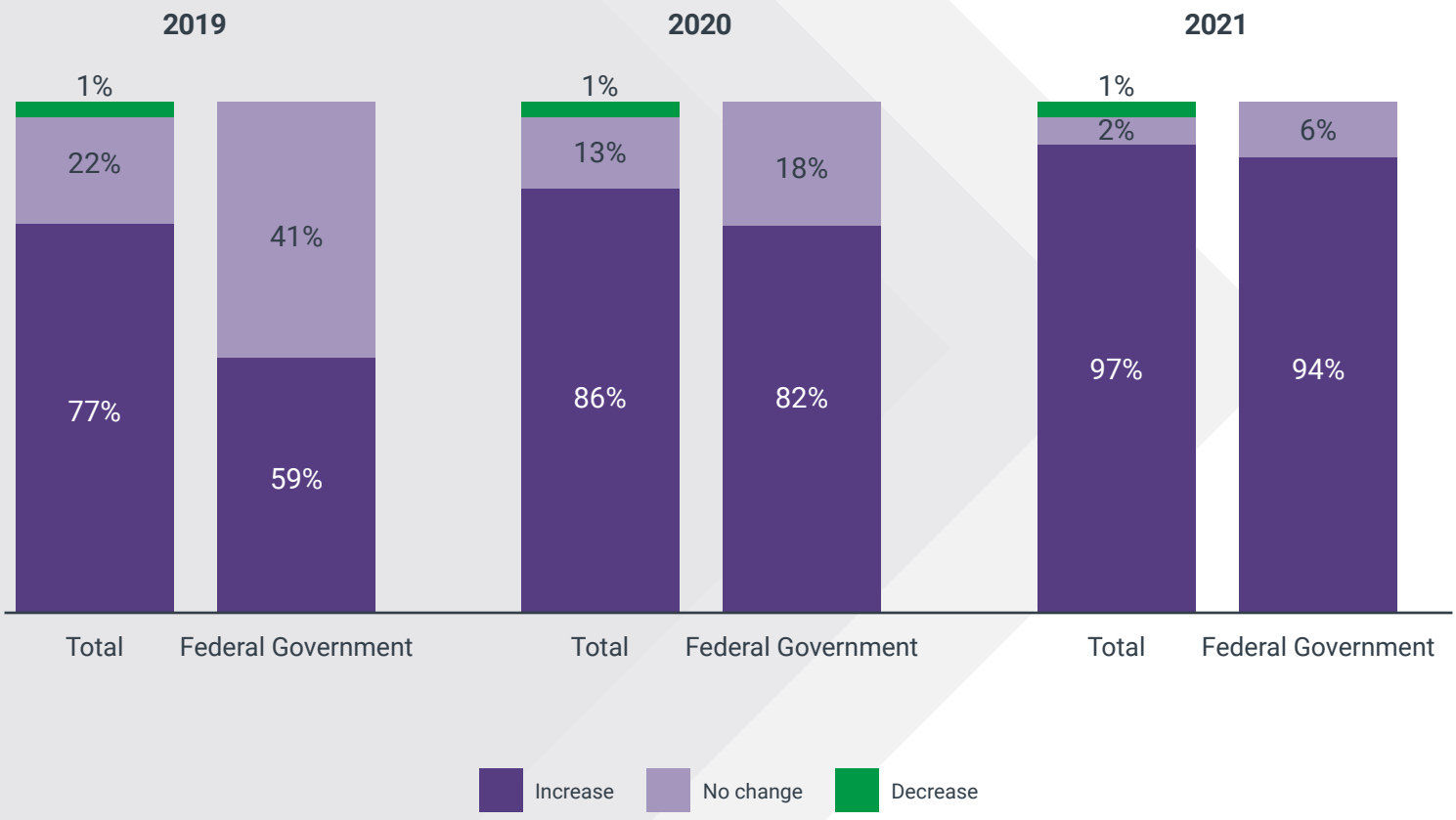
When validating network device configuration settings, all (100%) of federal organizations only assess their firewalls. Firewalls are not sampled. Each and every firewall is assessed, according to federal government respondents. These findings are largely consistent with the rest of the survey population, with most focusing on all firewalls, and only firewalls.

This finding suggests that there is cross-sector agreement that sampling is not best practice. It also highlights that most organizations rely on perimeter-only defenses. Only 4% of the cross-sector total, which didn't include any federal government organizations, assess their switches and routers as well as their firewalls, which according to Zero Trust best practice, is essential when it comes to preventing lateral movement across networks.

This survey reveals that all federal government organizations, despite their efforts to secure their firewalls, remain exposed to the potentially significant and unidentified risks that misconfigured routers and switches pose to network security. And in effect, they are still only sampling their fleet of network devices, which is an inherently risky approach to configuration security.

Budget appears to be a limiting factor in risk mitigation

Q7. How much has your organization's budget for network configuration validation activities increased each year?

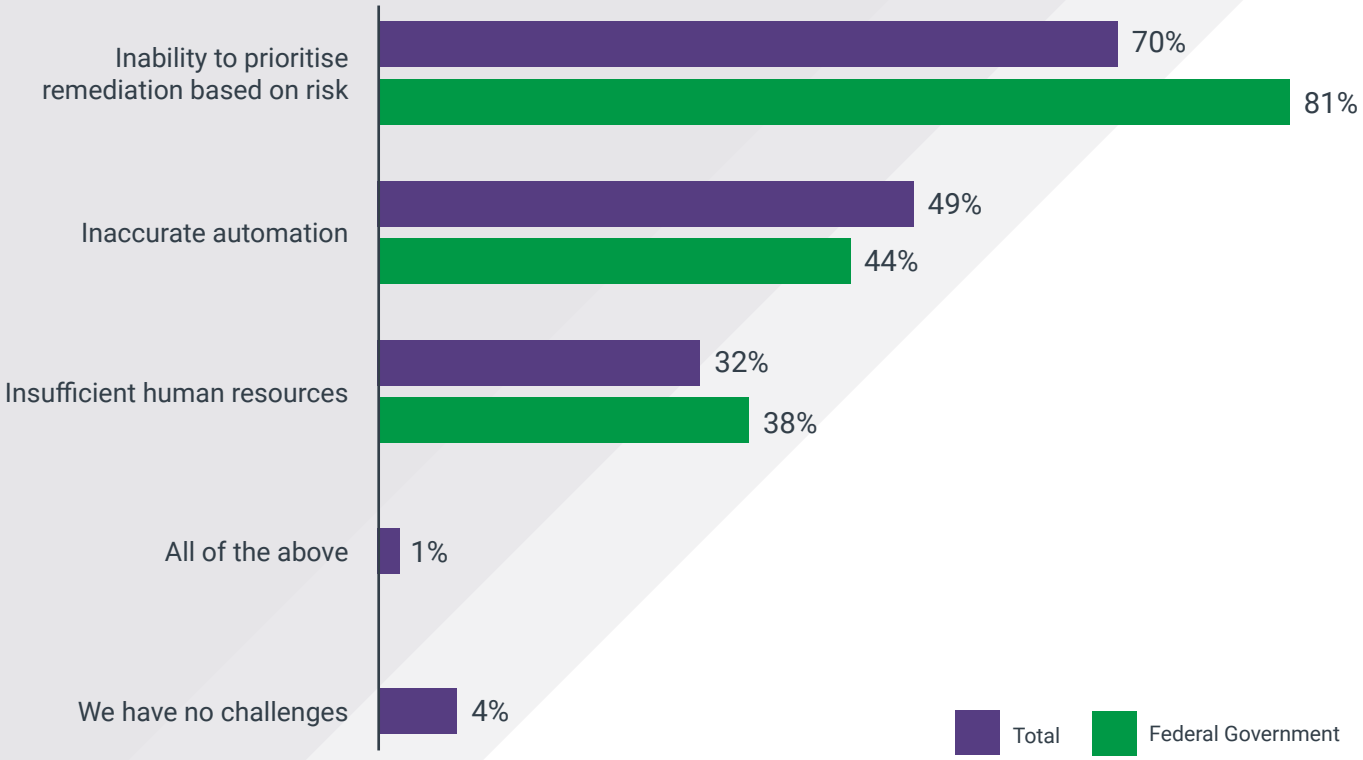


The budget set for network configuration risk management in federal government is, on average, just 3.2% of the total IT budget. This is consistent with cross-sector findings.

Again, in line with the rest of the survey respondents, federal government representatives shared that their budgets have increased, especially in the last two years, but it is reported to have had little effect on the number of misconfigurations identified. Half of all organizations see the number of critical misconfigurations they have discovered as unchanged since last year.

It is perhaps not surprising given budget limitations that all federal government respondents reported that they face a number of challenges in meeting security and compliance requirements.

Q8. What are the main challenges with meeting your organization security and external compliance requirements?



Interestingly, a lack of skilled resources is typically the number one challenge cited in cyber, yet in this survey, inaccurate automation, and an inability to prioritize security actions based on risk are reported as more significant issue. Cross-sector, 70% reported it as the biggest challenge, rising to a sizeable 81% of federal government respondents. Here, it is important to note that insufficient resources could potentially be a more significant challenge if:

- Configuration assessments were performed more frequently than annually/ bi-annually, and
- Switches and routers were assessed, along with firewalls.

Of course, this would, in turn, increase the need for investment in accurate and risk prioritized detection and remediation automation. And implementing such automation would likely have an adverse impact on the number of misconfigurations reported by network teams. But this would be an easy trade-off for teams that are investing in more proactive security to:

- Detect every misconfiguration in the network, in a timely manner, and
- Prioritize remediations based on criticality to security and/or compliance.

So, the top three network security challenges reported remain inextricably linked. While further federal government research would be required to explicitly determine whether budgets are the reason why all network devices are not assessed more frequently, it is a safe assumption that this is the case when considering the historic compliance frameworks to which these organizations needed to adhere. It also stands to reason that these budgets will need to increase significantly to enable organizations to adopt Zero Trust best practices moving forward.

Risk and remediation prioritization automation is a challenge
In answer to an earlier question in the survey, 71% of federal government respondents reported that their network security tools meant they could categorize and prioritize compliance risks 'very effectively'. This finding seems at odds with the fact that 81% report an inability to prioritize remediation based on risk as a top challenge when meeting security and compliance requirements. (Interestingly, the same contradiction was highlighted in each of the sectors surveyed).

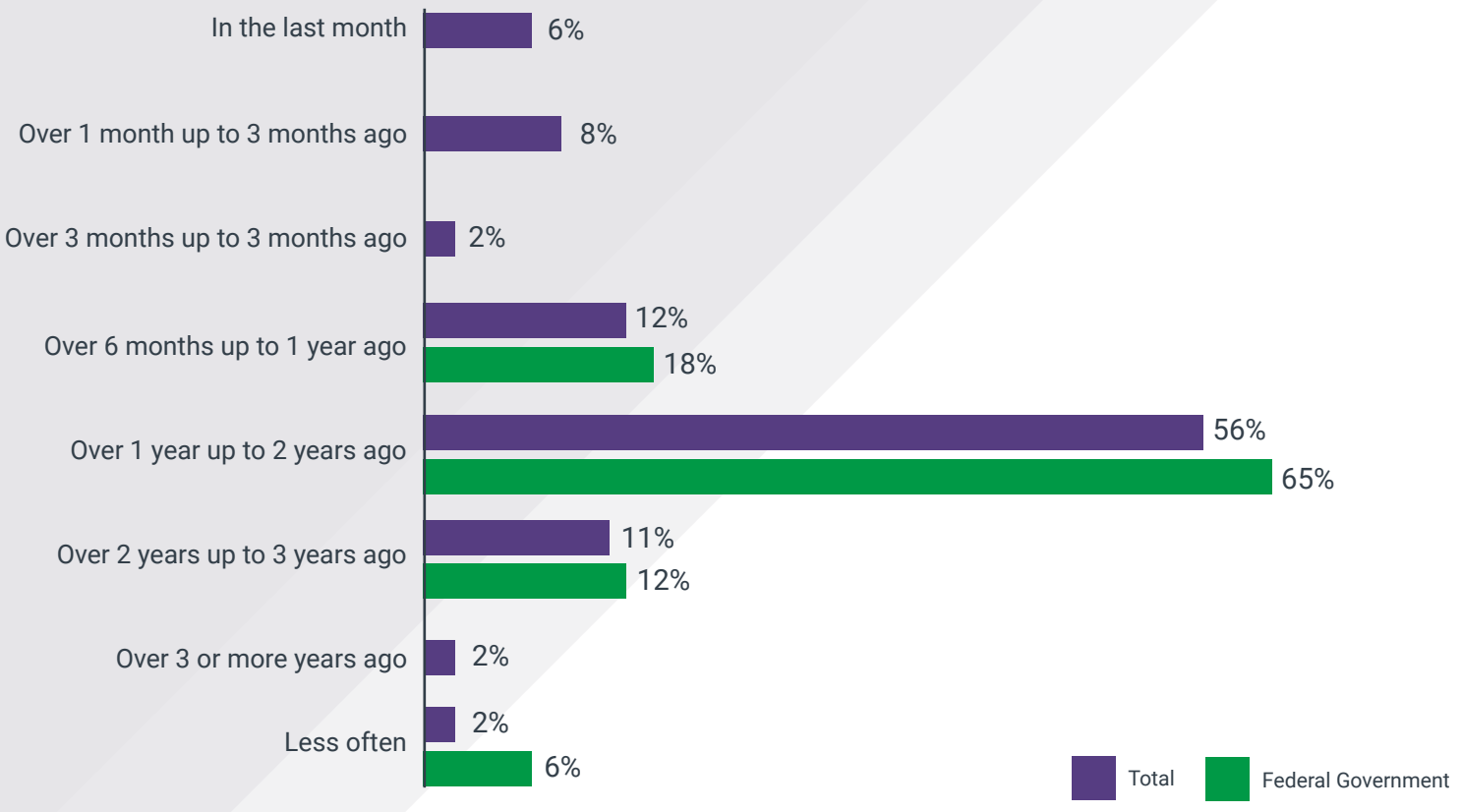
Again, this anomaly points to two possible issues with current security and compliance automation solutions. Firstly, while considered effective at prioritizing compliance risks on an annual or bi-annual basis, current solutions do not support continuous risk prioritization and mitigation - which is what compliance frameworks are now recommending. And secondly current tools do not provide the necessary insight to fix the compliance issues they detect and to automate remediation workflows. Which is how organizations can deliver security from compliance.

Calculating risks:

A closer look at misconfigurations

Please note, that this next set of findings needs to be considered in the context of the limitations with inaccurate automation and inability to prioritize remediation based on risk, outlined in the previous section, as respondents were asked to share information about the severity of the misconfiguration risks their teams have detected in the past 12 months.

Q9 When was the last time a network misconfiguration was identified?



Calculating risks: (contd)

Most respondents within the federal government sector reported identifying a critical configuration issue between one and two years ago (65%) while 18% said they had done so in the last year. Most of these configuration issues were rated between 3-5 on a scale of 1-10 (1 = not at all serious, 10 = very serious) for severity and were, the survey says, typically fixed within two days.

These findings are not surprising, as the majority of federal government respondents reported conducting firewall configuration assessments on an annual, or biannual basis. Therefore, it is unlikely that critical misconfigurations would be picked up more frequently in firewalls than on an annual basis, and any critical risks to router and switch security would remain undetected in 100% of cases.

Consistent with the cross-sector average, misconfigurations were reported to have be mitigated within two days of detection. However, the fact they could have resided on the network for one to two years, is a likely cause for significant concern. While mean time to remediate/repair (MTTR) is a vitally important metric, the mean time to detect (MTTD) combined with MTTR is a more accurate quantification of an organization's security posture. Indeed, configuration assessment practices that reduce both MTTD and MTTR are needed to inform risk remediation strategies and defend networks against preventable attacks.

Conclusion and recommendations for federal government

In the past, vulnerability management was considered robust if it comprised effective network segmentation as a mitigating control to support regular software patching and annual perimeter (firewall only) configuration assessments. Rarely were organizations required to validate that these practices delivered consistent cyber hygiene to comply with regulatory frameworks.

However, as a result of security breaches increasing in impact, frequency and profile, security and compliance experts have recognized that these historic practices are no longer adequate. Therefore, security and compliance best practice is shifting to reduce sampling and increase the cadence of assessments of all network devices, not just perimeter and endpoints.

As important as firewalls are, routers and switches play an equally vital role in effective network segmentation, which is a fundamental mitigating control to reduce the attack surface by stopping lateral movement across networks. These security measures are especially valid to defend the network from less sophisticated attacks. It's why Zero Trust principles and frameworks – and increasingly compliance requirements across all sectors – stress the need to assess all changes to routers and switches, as well as firewalls, to continually ensure that organizations effectively minimize their attack surface. And it's why leading organizations are now changing the way they approach configuration security and vulnerability management.

However, in times of change, there is often a disconnect between the way things are currently, and how they should be. So, it's perhaps not surprising that the survey responses across all sectors suggest a disconnect between the perception of network security, and the reality in the majority of cases, where:

1. Switches and routers are not checked for misconfigurations as part of annual audits – equating to security and compliance by sampling, which is an inherently risky approach

2. The frequency of assessments is annual, meaning that exploitable configurations in firewalls may reside on networks, undetected, for up to 364 days

3. By default, organizations cannot comply with risk management and/or security control frameworks that recommend abandoning sampling, and regularly assessing all network devices; and

4. Exploitable vulnerabilities in the form of critical misconfigurations in firewalls, and particularly in switches and routers, are currently an unquantified risk for the majority of organizations.

Ultimately, critical risks that compromise the confidentiality, integrity and availability of data, systems and services are considered intolerable by the vast majority of Network Risk Owners. This is especially the case for high-profile targets like federal government organizations that also need to secure their networks against nation state attacks. And so having full visibility of misconfigurations and the risk they pose to network security is essential in order to effectively prioritize remediation workflows.

As this survey indicates, it's not simply a case of federal organizations investing in accurate automation to deliver assessment and risk and remediation prioritization across all their firewalls, switches and routers. It also requires a shift in mindset to one of Zero Trust. Where Network Owners do not trust that device configurations pose no risk to the network between annual audits, but proactively and continuously verify that these configurations remain compliant, and therefore secure. Only then will federal government organizations deliver security from compliance.

To discuss the findings from this research, or to understand more about how Titania can help your federal government organization make the shift from ad-hoc to continuous assessment of your firewall, switch and router security and compliance – please get in touch: marketing@titania.com

About

About Titania

Based in the UK and Arlington, VA, Titania delivers essential cybersecurity automation software to thousands of organizations including 30+ federal agencies within the U.S. government, global telcos, multinational financial institutions, and the world's largest oil and gas companies. Specializing in the accurate security and compliance assessment of networking devices – firewalls, switches and routers – Titania helps organizations defend their networks from preventable attacks by identifying configuration drift and prioritizing the remediation of their most critical risks, first.

The company is best known for its award-winning solution, Nipper, which also overlays its security risk findings onto RMF assessments to assure compliance for CDM, DISA RMF, NIST, CMMC and PCI DSS. To meet the growing market need for continuous accurate, risk and remediation prioritized assessments, Titania is now focusing on scaling Nipper for enterprises to support their zero trust security strategies.

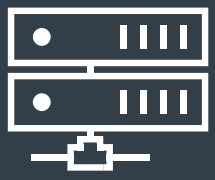
Visit Titania at www.titania.com

About Coleman Parkes Research

Coleman Parkes Research is a business to business (B2B) research specialist with first-rate experience across all verticals and global markets.

We undertake telephone interviews, online surveys, in-depth discussions and focus groups with senior level decision makers in companies of all sizes. Our in-house team experts ensure all clients' research projects are designed and structured to not only gather the right data but also generate prized insights that question the 'so what?' and drive effective business growth.





TITANIA
Assured Accuracy

Titania, Suite 600,
2451 Crystal Dr, 6th Floor,
Arlington, VA 22202