TITANIA
Assured Accuracy

The impact of exploitable misconfigurations on network security

A report on the current approaches to mitigating risks

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.

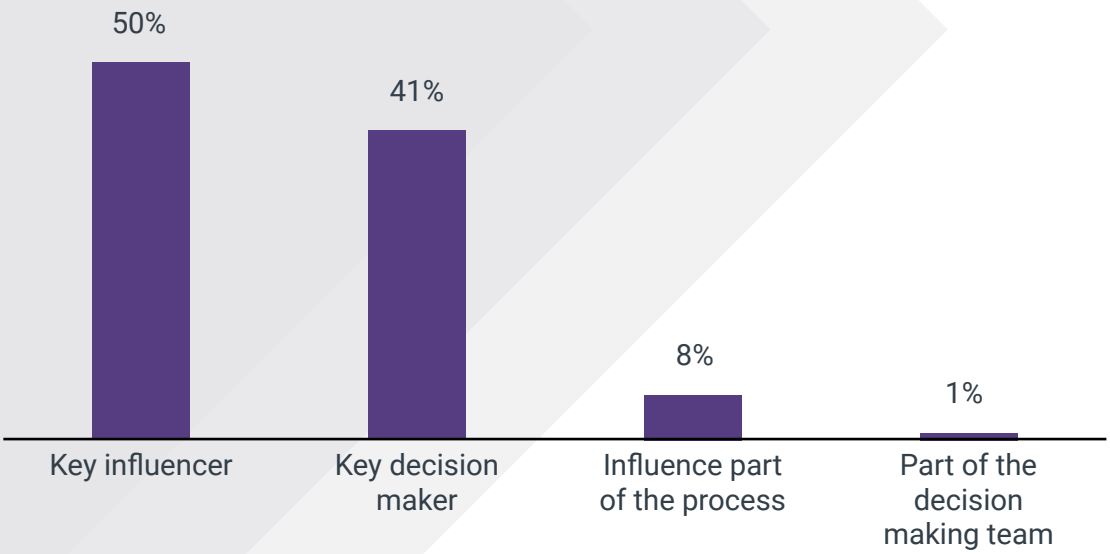
But increasingly, exploitable vulnerabilities, and how to prevent them, are back on the agenda. Particularly as recent attacks on critical national infrastructure organizations have utilized arguably less sophisticated tactics to exploit network vulnerabilities and compromise the confidentiality, integrity and availability of data, systems and services. 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.

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 hardening networks from the inside-out, making it as difficult as possible for intruders to gain entry and progress towards their goal by inhibiting lateral movement, is an essential defense strategy. 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, in order to prioritize the mitigation of exploitable vulnerabilities based on risk.

This kind of proactive security is key to protecting networks from preventable attacks. It acknowledges that security within the network boundary is as important as the security on devices forming the perimeter. The aim being for all devices to maintain a secure configuration that matches both network policy and functional intent, at all times. Indeed, some sectors are seeing this as a baseline for Zero Trust security, and why more and more organizations are now adopting a Zero Trust mindset.

Networks can change on a daily basis (typically through planned activity) resulting in configuration drift between audits. So, Titania wanted to understand more about how organizations are 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 160 senior cybersecurity decision-makers across the U.S. Military, Federal Government, Oil and Gas, Telecoms and Financial Services sectors. The survey asked how organizations currently detect and mitigate vulnerabilities in this part of the network and how confident they are that devices maintain a secure configuration at all times.

Network security role



Base: All respondants (160)

Total

Executive summary

This report presents an overview of how organizations across military, federal and critical national infrastructure sectors in the U.S. proactively find and fix exploitable vulnerabilities in their networks. Based on the insights provided by the CIOs, CTOs, CISOs, COOs, Heads of Networks, Network Security, and Network Operations leaders, who participated in the survey, the report highlights four key challenges that need to be addressed in order to protect organizations from preventable attacks, in line with best practices.

The task of defending networks against preventable attacks is no easy feat. 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 on a daily basis.

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. It’s why a consistent proportion of annual IT budgets are allocated to network configuration risk management across the sectors (around 3.4%), and why these budgets are increasing every year.

Overall, the survey found that security decision-makers are very confident about the security of their organization’s networks. Almost every respondent says that they are meeting their security and compliance requirements, and all without exception believe that their network security tools are at least ‘fairly effective’, allowing them to categorize and prioritize compliance risks.

Executive summary (contd)

Interestingly, the same respondents also reported that their organizations do not analyze switches and routers when checking for misconfigurations; that checks are typically performed on an annual basis; and that budgets have increased year on year, but this has little to no impact on the volume of critical misconfigurations detected on their networks.

So, whilst respondents estimated that misconfiguration risks, all levels combined, are costing their organizations around 9% of their revenue - the true cost is likely to be much higher.

The survey data also clearly indicates that for all organizations budget is a limiting factor in misconfiguration risk management, but:

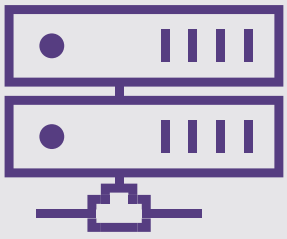
1. Validating network configurations is a top three priority for organizations,
2. The shift from ad-hoc to continuous assessment of configuration risks is strategically important,
3. The inability to prioritize remediation based on risk is the biggest challenge.

Read on to find out what this means in practice...

Self-reflection:

Respondents are confident that their current networks are secure

During the survey, respondents were 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.

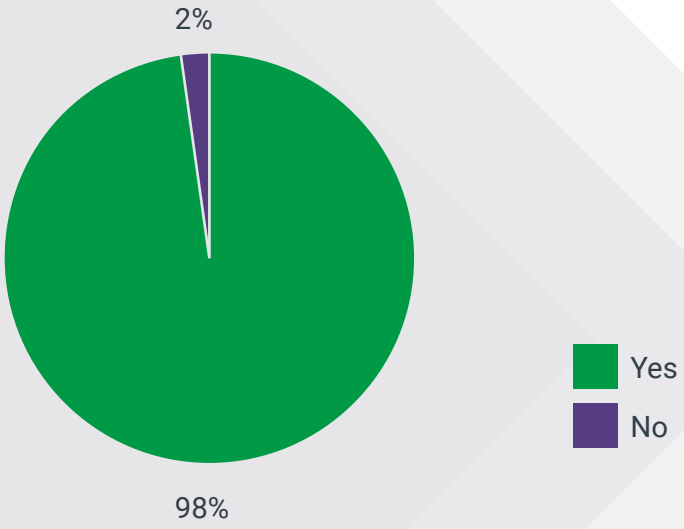


The survey started with questions regarding their organization's approach to network security and compliance.

Self-reflection: (contd)

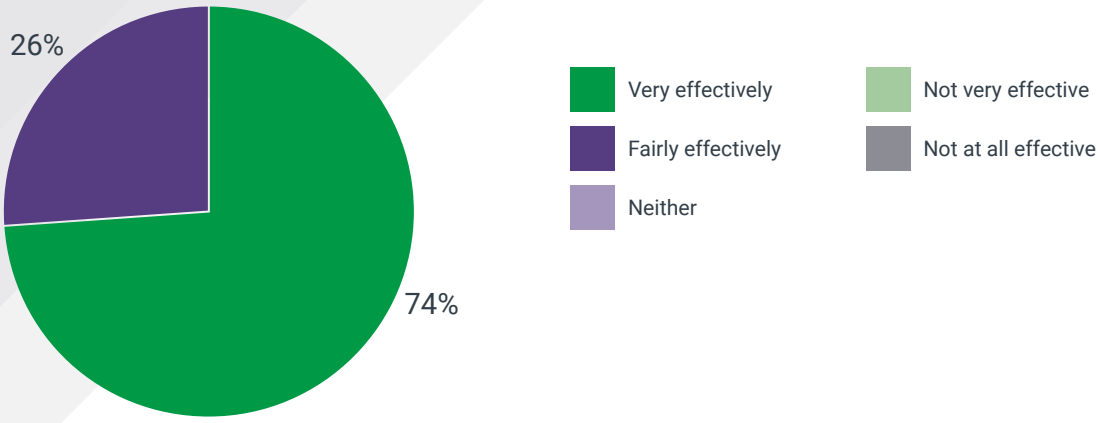
Organizations report they are meeting security and compliance requirements
Respondents are, on the whole, very confident that they are meeting their corporate security and external compliance requirements. This is an important finding when more than 75% of respondents across all sectors agree that their organization relies on compliance to deliver security.

Q1 Are you meeting your corporate security and external compliance requirements?



Three-quarters also said that their network security tools meant they could categorize and prioritize compliance risks very effectively, and the rest said they could do so fairly effectively. No respondent rated their network security tools as less than "fairly effectively".

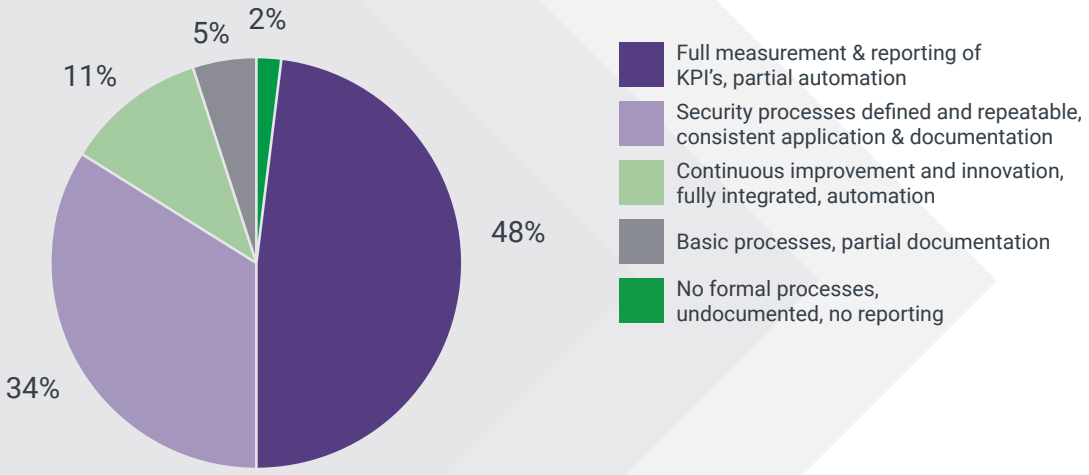
Q2 To what extent do your network security tools allow you to effectively categorise and prioritise identified security and compliance risks?



Self-reflection: (contd)

The survey revealed similar levels of confidence when 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 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?

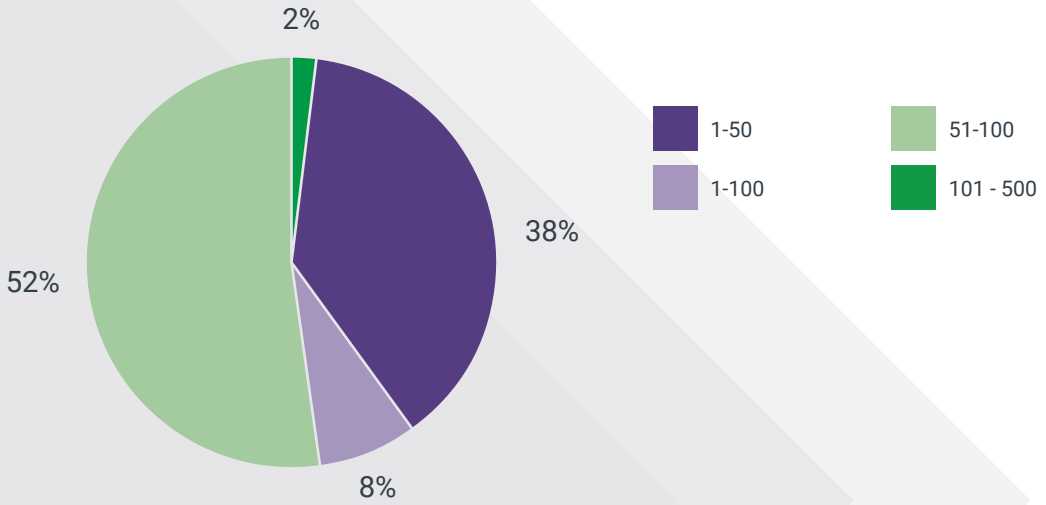


Nearly half (48%) said that they had full measurement and reporting with some automation whilst 34% said that their security processes were at least documented and repeatable. Another 11% said that they had continuous improvement in place with automation, leaving just 7% with either no formal processes, or the most basic of processes.

Respondent data sets, segmented by sector, are available on request **here**

Self-reflection: (contd)

Q4 How many misconfigurations in total have been identified in the past 12 months?



Validating network configurations is a top three priority
Validating network configurations is seen as a top three consideration for 92% of network security teams. Almost every single organization also confirmed that validating network configuration security was a part of their overall risk management strategy.

The processes that organizations have in place means that they are picking up misconfigurations—an average of 59 in the last year. Of which, respondents reported that five 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, estimating that misconfiguration risks, all levels combined, are costing them around 9% of their revenue. They also estimate that around 13% of resources from various teams are used for network configuration risk management activities.

Deep-dive:

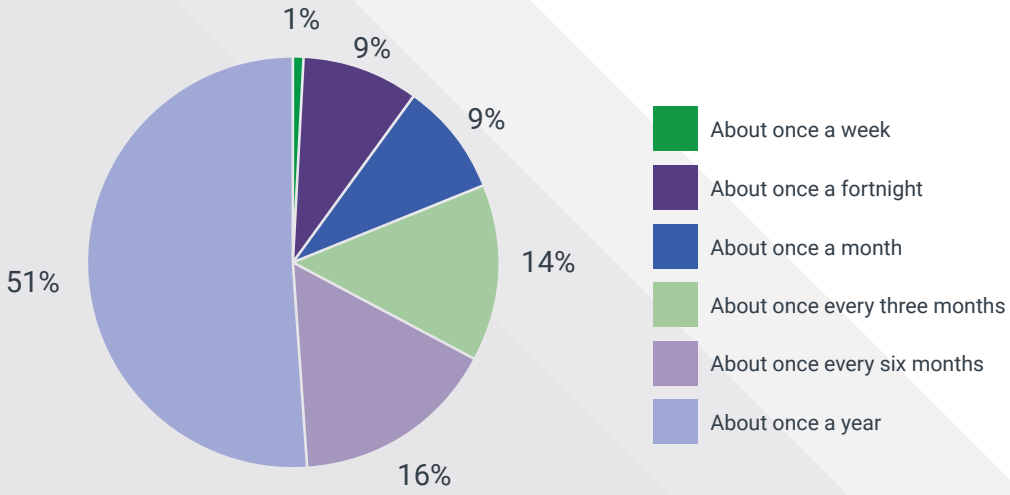
Understanding current configuration assessment processes

Networks can change on a daily basis. It's why many risk management and security control frameworks/programs - including the Payment Card Industry's Data Security Standard 4.0 and the United States Government's Continuous Diagnostics and Mitigation (CDM) 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 significant operational and business/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.

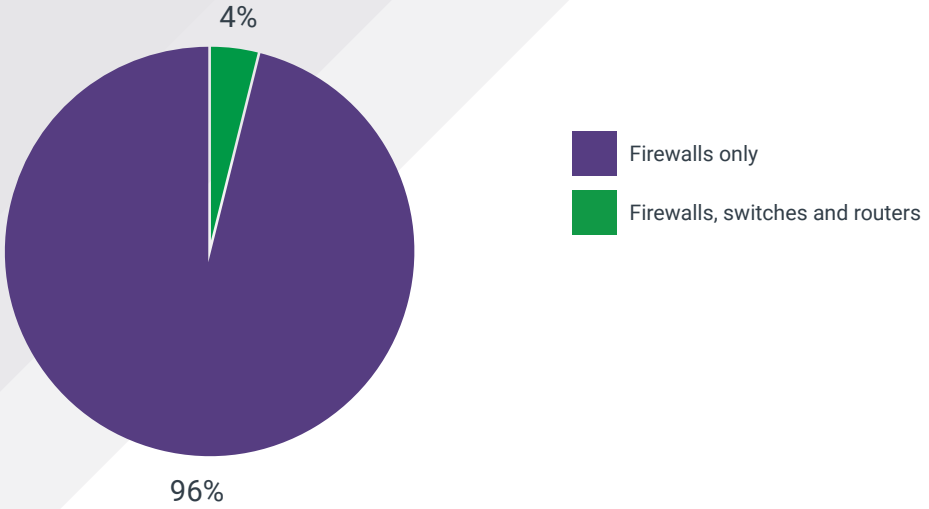
Deep dive: (contd)

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 organizations
In a pattern that was similar no matter the size or sector of organization, most (51%) assessed the configuration of network devices on an annual basis. Less than 20% assess them within a monthly cycle; of which only a tiny minority (1%) reported a weekly cadence.

Q6 When scanning and performing vulnerability and configuration assessments, do you assess:



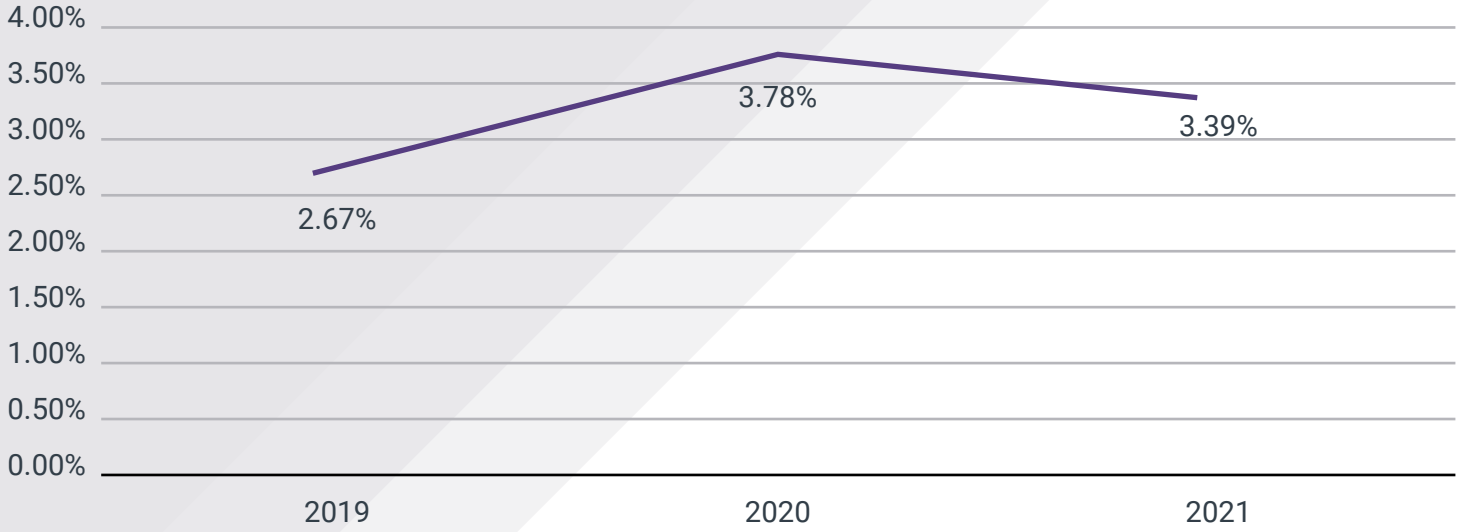
Almost all organizations only assess their firewalls
When validating network device configuration settings, almost all (96%) of organizations only assess their firewalls, and 94% choose not to sample these devices, but to test them all.

This finding suggests that organizations agree that sampling is not best practice. It also highlights that most organizations rely on perimeter-only defenses. Just 4% 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 most 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 of your organization's budget for network configuration validation activities increased each year?



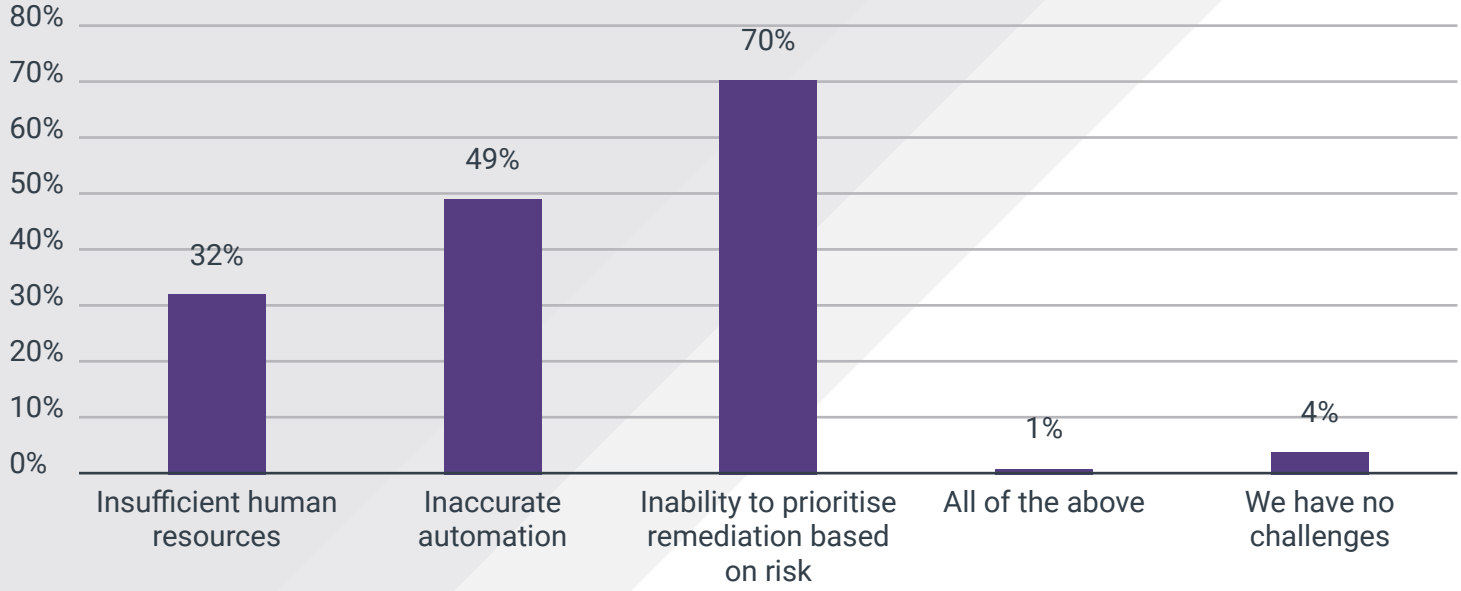
Deep dive: (contd)

The budget set for network configuration risk management is, on average, just 3.4% of the total IT budget. This is potentially a controversial finding when considering the previously mentioned estimation that misconfigurations cost organizations as much as 9% of their revenue.

Respondents shared that their budgets have increased, especially in the last two years, but it is reported to have had little effect. Half of the 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 but 4% of respondents reported that they face a number of challenges in meeting security and compliance requirements.

Q8 What are the main challenges with meeting your corporate 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 based on risk are reported as more significant issues by 70% of 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. However, 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 these top three network security challenges remain inextricably linked.

Whilst further 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, 75% of 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 70% report an inability to prioritize remediation based on risk as a top challenge when meeting security and compliance requirements.

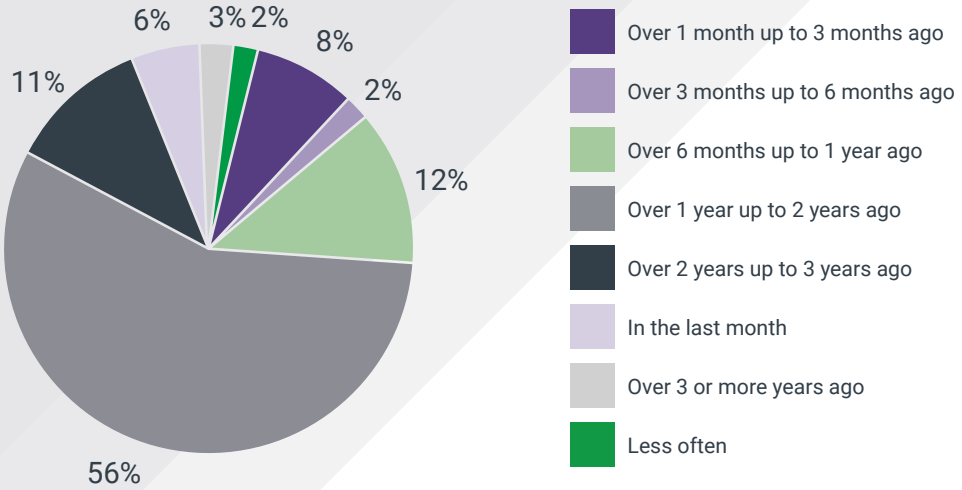
Again, this anomaly points to two possible issues with current security and compliance automation solutions. Firstly, whilst considered effective at prioritizing compliance risks on an annual or bi-annual basis, current solutions do not support continuous risk prioritization and mitigation - which is 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.

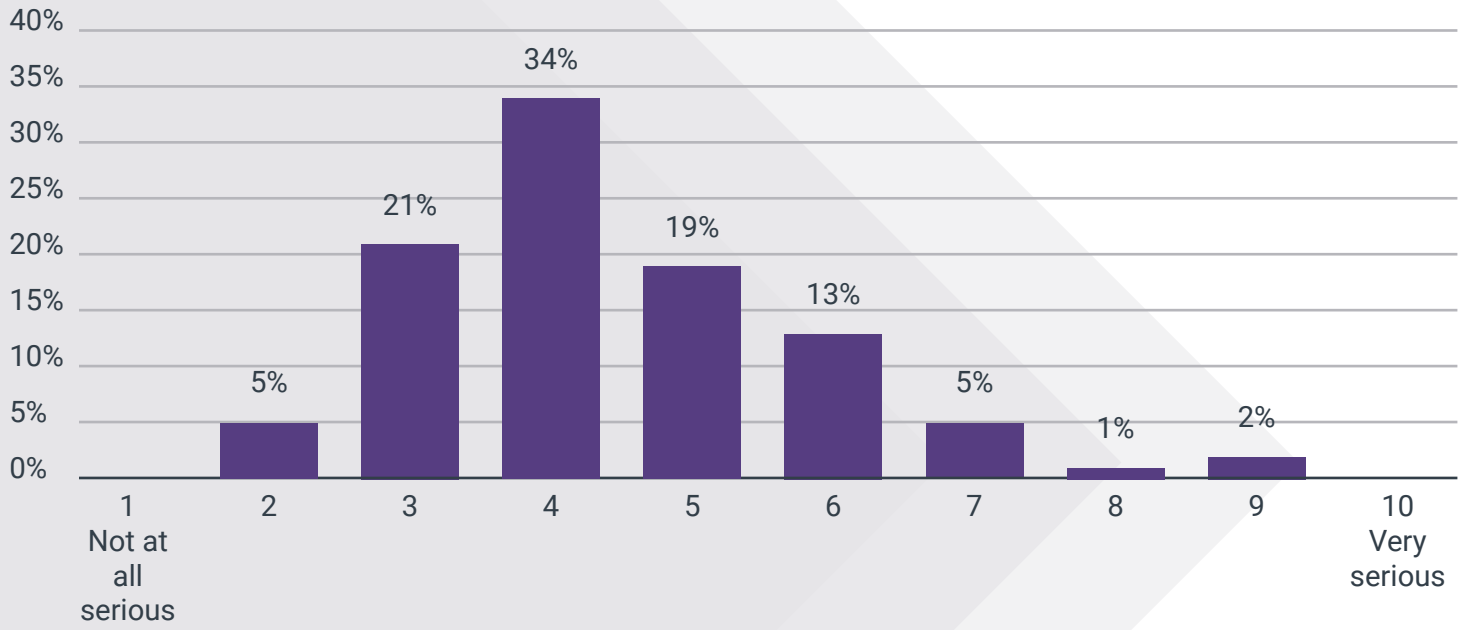
Q9 When was the last time a network misconfiguration was identified?



Most respondents reported identifying a critical configuration issue between one and two years ago (56%) while 28% 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.

Calculating risks: (contd)

Q10 How serious was the last network misconfiguration that was identified?



These findings are not surprising, when the vast majority of respondents reported conducting configuration assessments on an annual, or biannual basis and typically cover firewalls, but not routers and switches. Therefore, it is unlikely that critical misconfigurations would be picked up more frequently in firewalls than on an annual basis, and any critical risks on routers and switches would remain undetected in 96% of cases.

As impressive a statistic it is that misconfigurations are mitigated within two days of detection, the possibility that they could have resided on the network for *one to two* years, however, is a likely cause for significant concern. Mean time to remediate/repair (MTTR) is a vitally important metric, however, 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

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. This is why 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 its why leading organizations are now changing the way they manage vulnerabilities.

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 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. 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 organizations investing in accurate automation to deliver continuous assessment and risk and remediation prioritization across entire networks. 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, but proactively verify that they remain compliant at all times. Only then will organizations deliver security from compliance.

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

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.

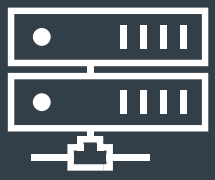
Visit Titania at www.titania.com

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