panaseer

Panaseer 2020 Financial Services Security Metrics Report

Contents

Introduction 3

Key findings 4

SECTION 1: **The value of metrics** 5

Factors that are impacting CISOs ability to deliver metrics at scale 6

SECTION 2: **When trust breaks down** 8

Top challenges when producing security metrics 9

Firms security programmes lack maturity 10

SECTION 3: **A demanding audience for metrics** 11

SECTION 4: **Metric mayhem** 13

SECTION 5: **The road to metric maturity** 14

SECTION 6: **Getting it right** 15

The last word 16

Methodology 17

Introduction

There are plenty of things to keep today's financial CISOs awake at night. Try the **tens of billions**[1] of cyber-threats detected each year. Or the rapid development and dissemination of new tools and techniques, on a cybercrime underground **said to be worth**[2] $1.5 trillion annually. That's not to mention a growing corporate attack surface expanded by digital transformation and cloud investments. And an escalation in complex reporting requirements for a patchwork of multi-jurisdictional regulations.

In response, many security leaders are investing in a broad sweep of cross-domain tools which have given their organisations a misguided sense of confidence. More tools don't mean better security. Instead, they can lead to specific challenges such as hindered visibility and measurement of the security posture, especially if the organisation has no way to gain centralised insight. Many tools could be deployed and shown to be performing well on the same assets (be it devices, applications, people, accounts or databases). However, without consolidated visibility it is difficult to uncover previously unknown assets and pin-point duplication of coverage insights on known assets and understand enterprise wide cyber posture with the business context required for effective desicion making.

So, what's the answer?

At the heart of any effective security programme are metrics: the objective measurements that answer key questions about how well the organisation is managing controls coverage and security risks. When done right, metrics help enterprises create a stronger security posture by ensuring a control failure does not turn into a security incident. But finance sector CISOs are struggling to know what to measure, and whether their metrics are accurate.

Plus, they are becoming overwhelmed with the sheer volume of measurements that modern compliance regimes and internal stakeholders demand.

To find out more, Panaseer commissioned independent research company Censuswide to interview over 400 senior security leaders and their teams working in large companies within the financial services industry.

We found that trust in the data is the biggest challenge for teams producing security metrics, and is therefore a major roadblock to building an effective security programme.

Why? Because too many attempts to develop these metrics are founded on error-prone, manual, point-in-time processes.

As various stakeholders' requests for security metrics bombard stretched security teams, CISOs will increasingly find these manual methods no longer fit-for-purpose. Manual processes also create challenges around speed-to-comply with request deadlines, and the ability to substantiate findings with the details required. Going forward, senior security leaders will need to focus on building out programmes in which metrics can be automated, continuously measured and accurately aligned to business processes.

[1] 2019 ANNUAL SECURITY ROUNDUP, The sprawling reach of complex threats, February 2019

[2] Understanding the Growth of the Cybercrime Economy, Researched and written by Dr. Mike McGuire for Bromium Inc, April 2018

Key findings

Metrics have become increasingly important for security leaders.

Security metrics are central to a successful cyber programme. **96%** of security leaders use metrics for measuring cybersecurity posture and reporting to a growing group of stakeholders, such as the board, regulators, auditors and customers.

The security team is facing an overload of requests for metrics.

This overload of requests can also have a serious knock-on effect as security teams divert resources from investigation and response to emerging threats. For example, auditors demand data most frequently at every 10.4 days on average, per month, followed by the regulators at every 11.4 days.

Teams are wasting an inordinate amount of time processing and reporting on metrics.

Security teams are spending more than 290 work hours per month on reoccurring and ad-hoc reporting to various stakeholders (outside of security department); most reporting time spent is for IT (44 hours or 5.5 days) and lines-of-business (43 hours or 5.4 days).

Many security leaders don't trust the data they use.

Over a third (**37%**) of security leaders said that the biggest challenge in creating metrics to measure and report on risk was 'trust in the data'.

Reliance on manual processes fuels the metrics mistrust.

Nearly **60%** of security leaders are reliant on spreadsheets to calculate security metrics, while **53%** use custom scripts.

Security leaders are aiming for better 'metric maturity'.

Nearly half describe their programme as basic, elementary or intermediate. However, two-thirds (**65%**) claim they want to be at upper intermediate or advanced stages for all audiences by 2021.

SECTION 1:

The value of metrics

Let's put things into context. **Gartner predicts**[3] that enterprises are expected to spend $170.4 billion on security by 2022. Financial CISOs are spending big in response to a proliferation of cyber-threats, rigorous compliance requirements, and a widening corporate attack surface. According to **research that we ran in 2019**[4], the average security team is using over 50 tools today, in areas as diverse as: vulnerability management, endpoint detection and response (EDR), identity and access management (IDAM), privileged access management (PAM), patch management, application security, and user awareness training.

But alongside this increasing spend, breaches are increasing, and so too are the cost of attacks. The disconnect cannot be simply explained by savvier attackers, especially given that Gartner also cited that **99%** of the vulnerabilities exploited by the end of 2020 will not be zero days, but those known by security and IT professionals at the time of the incident.

The core underlying problem as to why no significant improvement has been made in enterprise security is a lack of centralised measurement of safeguards and controls around our assets.

Ultimately, these organisations need metrics to provide much-needed visibility into their controls to help decision-makers understand where they're most exposed to risk and how to improve performance. No wonder **96%** of the survey respondents told us metrics are currently used in the organisation to measure cybersecurity posture.

The bottom line is - you can't secure what you can't measure. And you can't make effective, informed decisions if you're not basing those decisions on accurate, complete and continuous insight into the effectiveness of security controls.

Metrics are needed to support a wide range of activities in today's financial organisations, and to report to a wide range of stakeholders. When used effectively, metrics can help CISOs prove the value of existing strategies and bolster their case for greater investment.

What is the primary use of security metrics in your organisation?

[3] Forecast Analysis: Information Security, Worldwide, 2Q18 Update, Gartner, September 2018

[4] Panaseer Security Leader's Peer Report, June 2019

Factors that are impacting CISOs ability to deliver metrics at scale

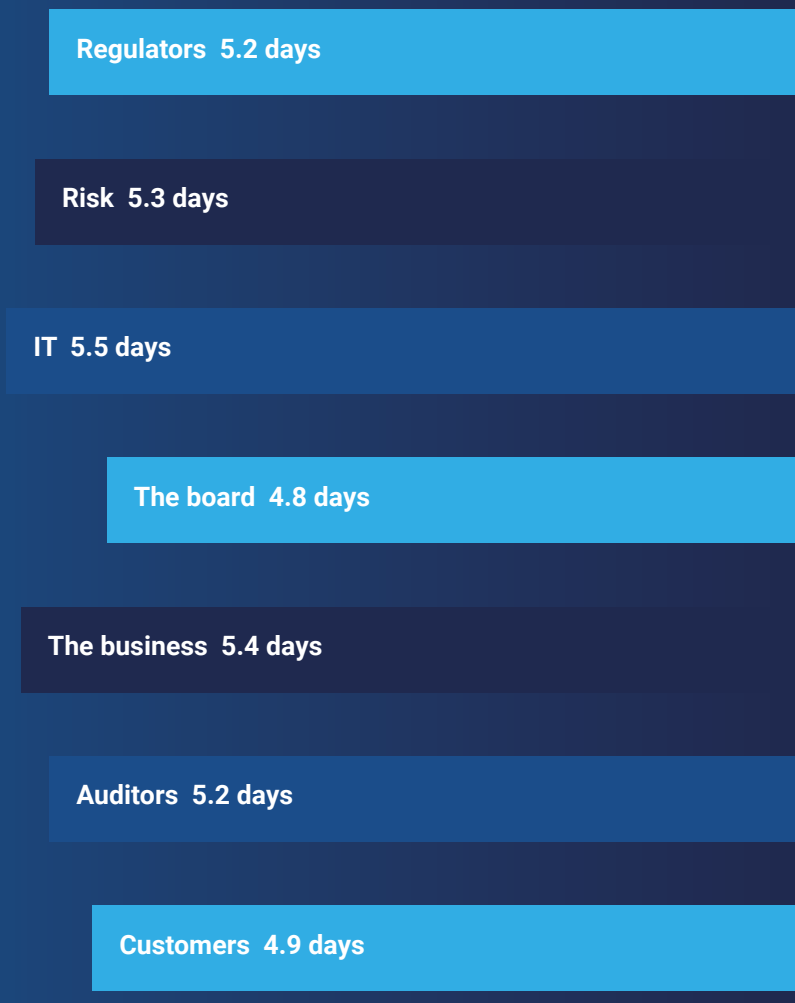
Whilst financial CISOs understand the value of metrics, there are a number of factors that are impacting their ability to deliver these at scale, including:

Not enough time
Security teams spend an inordinate amount of time conducting extensive data engineering and reporting work to understand the cybersecurity posture of an organisation. This is a long, arduous process. On top of this, security teams in financial institutions spend a lot of time to create and prepare reports for various stakeholders.

On average, per month, the team is allocating the following time to recurring and ad-hoc reporting requests: regulators – 5.2 days, risk – 5.3 days, IT – 5.5 days, the board - 4.8 days, the business – 5.4 days, auditors – 5.2 days, customers - 4.9 days. This means that they spend in excess of 290 hours every month to produce reports for other stakeholders, not counting the time spent reporting on their day-to-day duties such as monitoring cybersecurity posture of the organisation.

Virtually every day there is someone in the security team working on recurring and ad-hoc reports for a stakeholder group. This is time that could be better spent investigating security incidents or addressing the sea of alerts they're drowning in.

The amount of time security teams allocate to metric requests per month



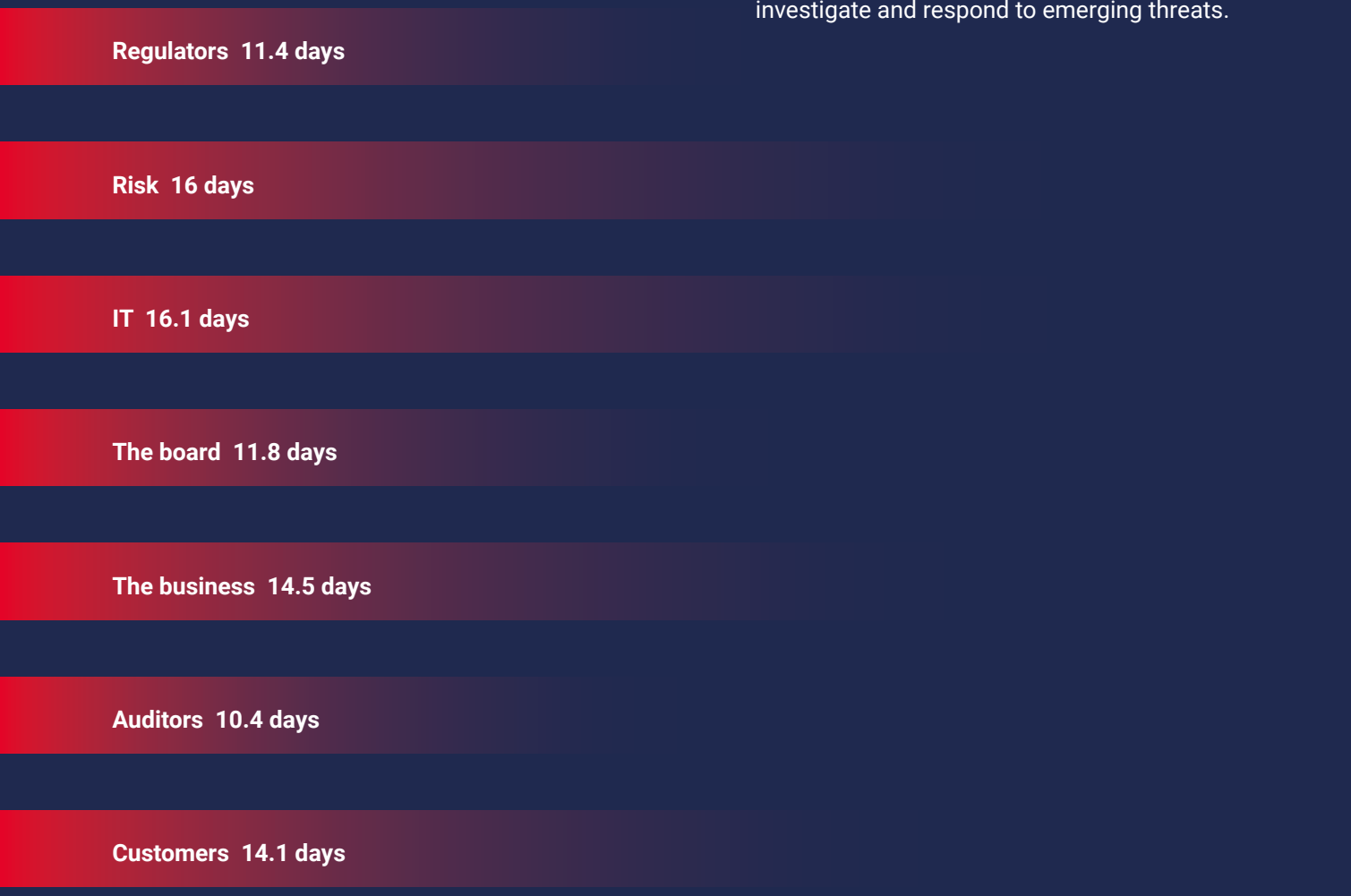
Too many requests
Auditors demand data most frequently, followed by the regulators themselves.

Across the board, there is a need for updated metrics almost twice a month or more.

The security team is getting requests from the following stakeholders at this level of frequency: regulators - every 11.4 days, risk teams - 16 days, IT - 16.1 days, the board - 11.8 days, the business - 14.5 days, auditors - 10.4 days and customers - 14.1 days.

This overload of requests could also have a serious knock-on effect if security teams aren't able to investigate and respond to emerging threats.

The frequency of requests from stakeholders



SECTION 2:

When trust breaks down

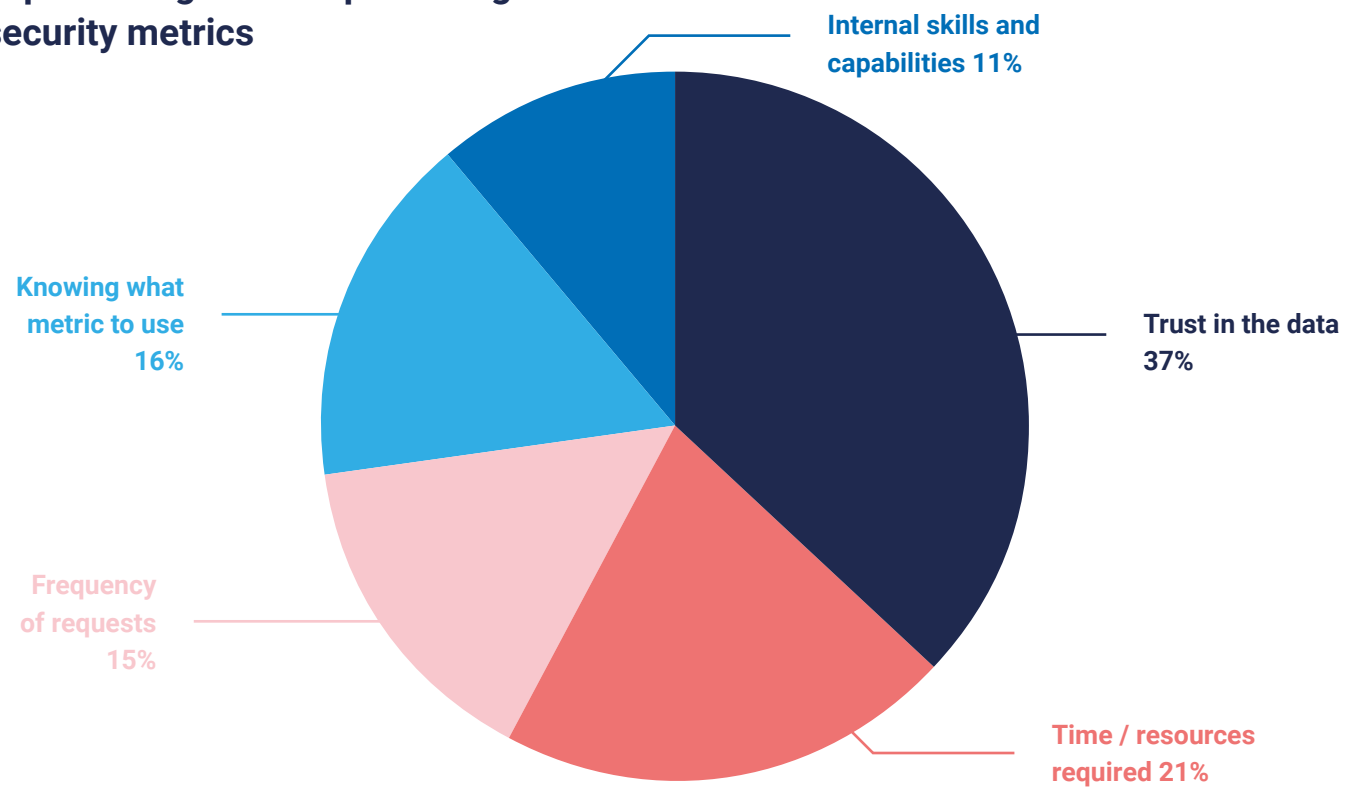
Security metrics themselves can be developed using various tools. But the type of approach organisations take can have a major impact on how fit-for-purpose their measurements are.

We found that nearly **71%** of respondents use in-house solutions and **60%** of respondents are using spreadsheets to calculate security metrics, while a similar number pointed to BI tools (**55%**) and custom scripts (**53%**). Though in-house solutions usually manage their tools centrally and share security and risk posture with other business units, they are still susceptible to issues mentioned below. These methods are relatively time and resource-consuming, prone to human error, and most are manual. Organisations use these processes because data around tool usage, effectiveness, and statuses are siloed in each individual tool. In the case of in-house solutions, the tools might be centralised, but they are still disjointed.

Without platforms that can unify the data for reporting, teams spend their time tabbing between tools and updating their own dashboards.

There are several key processes that are best left to automated tools. For example, entity resolution, where data from multiple sources is cleaned, normalised, de-duplicated, correlated, and aggregated to particular entities, and data triangulation, where triangulation of entities present in one source but missing from another leads to uncovering previously unknown assets.

Top challenges when producing security metrics



If metrics are being produced by manual, error-prone processes, then it's perhaps unsurprising that trust in the data they produce is the number one challenge cited by security leaders.

The problem appears to be particularly acute when presenting metrics to risk teams and servicing customers, where **37%** and **33%** respectively cited it as their top issue. Over a quarter (**26%**) of security leaders cited it in the context of regulatory reporting, where the stakes couldn't be higher.

If CISOs aren't confident in the data being produced, crucial gaps in visibility and controls may emerge which expose the organisation to serious cyber risk. Major regulatory fines and reputational damage could follow.

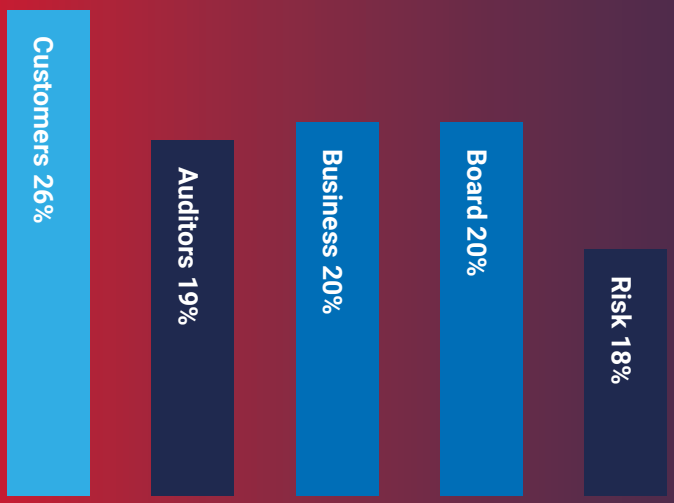
Interestingly, several of the other challenges provided by respondents also stem from the manual processes many organisations are using to develop their security metrics. These include the time and resources required, as well as having the right internal skills and capabilities.

The frequency of requests, which is a problem for over a sixth of respondents in the context of metrics for regulators and customers, is another symptom of this skills challenge.

Firms' security programmes lack maturity

Perhaps because of the widespread use of manual processes to develop metrics, around half of security leaders we spoke to describe their programme as basic, elementary or intermediate.

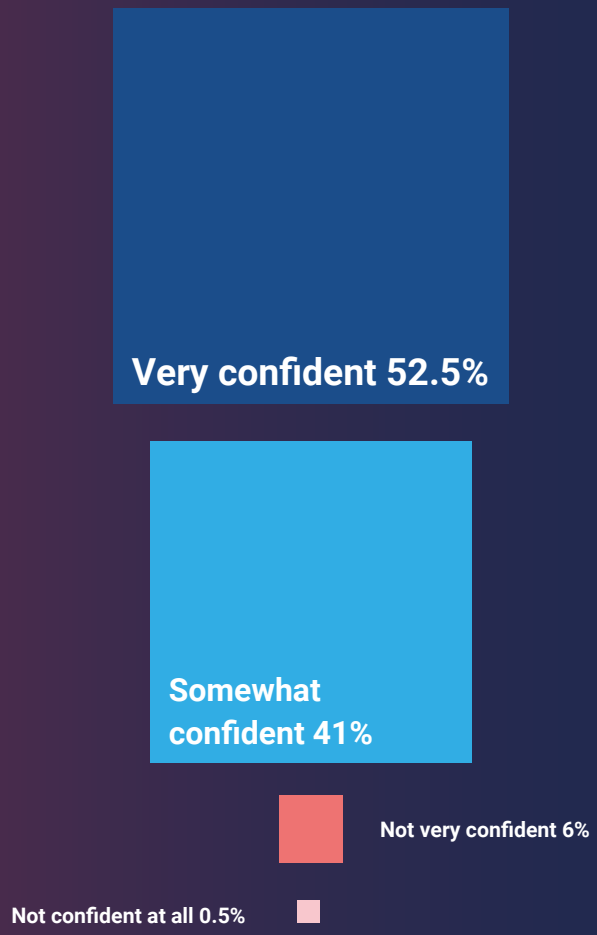
The percentage of security metrics produced for specific stakeholders at a basic or elementary stage of maturity



With regards to some audiences — such as risk teams (**18%**), the board (**20%**), the business (**20%**), auditors (**19%**) and customers (**26%**) — around a fifth or more of respondents claimed that their security metrics maturity was only at a basic or elementary stage. We'll discuss more about these groupings later in the report.

It is also telling that in the case of most audiences, only around half of CISOs surveyed said they were very confident in choosing the right security metrics in the first place. In the context of a risk and auditor audience, more were 'somewhat' or 'not very' sure than were 'very confident'.

How confident are you that you are measuring the right security metrics for different audiences?



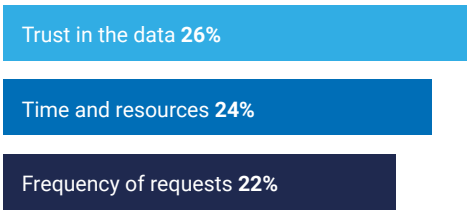
SECTION 3:

A demanding audience for metrics

As we've discussed, security teams in financial services companies are under increasing pressure to meet demand for metrics from all over the organisation.

The biggest challenges in producing metrics for regulators

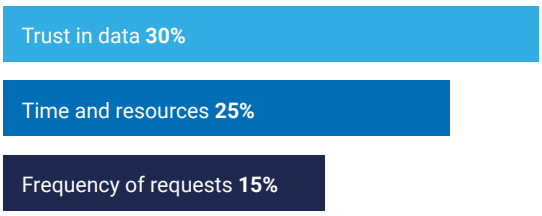
Regulators typically need security metrics to decide whether the security team is meeting its prescribed standards and processes. Security leaders report their biggest challenges in producing metrics for this audience as:



Nearly a quarter (**23%**) of CISOs say their metric maturity is no higher than elementary for this audience.

The biggest challenges in producing metrics for auditors

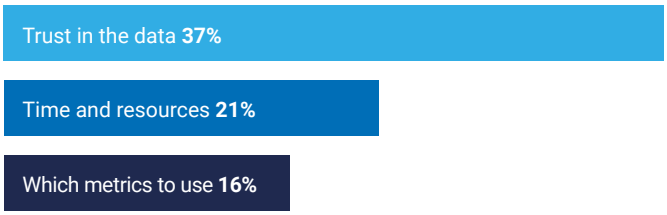
Like regulators, they need metrics to ensure proper process is being adhered to and the security team is meeting the standards it has set for itself. CISOs' biggest challenges for this group are:



29% of CISOs claim auditors demand data 4-6 times per week or every day. A fifth (**18%**) are at basic or elementary levels of maturity.

The biggest challenges in producing metrics for risk teams

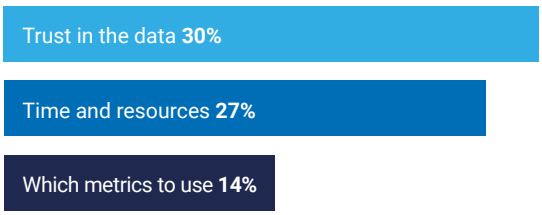
CISOs say the biggest challenges here are:



Some **29%** of respondents say risk teams demand data every day. Nearly a fifth (**18%**) say they are basic or elementary in terms of maturity.

The biggest challenges in producing metrics for IT

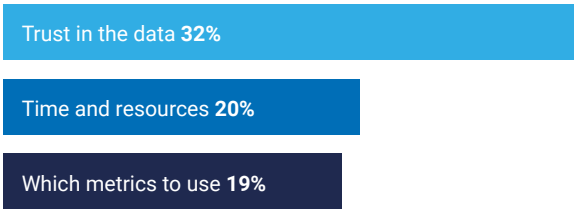
Respondents claim that their biggest challenges are:



Nearly half (**47%**) of CISOs say IT demands data on a daily basis or every 4-6 days. Nearly two-fifths (**37%**) are still not beyond intermediate levels of metric maturity for this audience.

The biggest challenges in producing metrics for the board

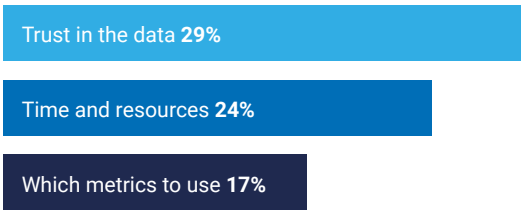
The board needs metrics to prioritise and see a clearer picture on the organisation's cybersecurity posture. It wants to understand security and the risk status of mission-critical parts of the business such as trading systems, payment processes, or systems that host PII. The biggest challenges are:



A third of CISOs (**33%**) say boardrooms want data at least 4-6 days a week and often every day. A fifth (**20%**) are not beyond elementary levels of maturity for these metrics.

The biggest challenges in producing metrics for the business

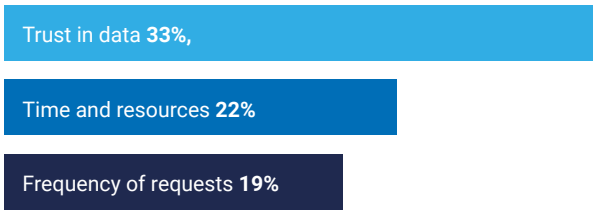
Like the board, these stakeholders need metrics that move away from technical language. CISOs say the biggest challenges in serving this audience are:



A quarter of security leaders (**24%**) say business audiences demand metrics on a daily basis. But a fifth are still at elementary maturity levels.

The biggest challenges in producing metrics for customers

CISOs say the biggest challenges producing metrics for customers are:



Over a fifth (**22%**) of respondents say this group demands data every day, rising to **41%** when including those who want it every 4-6 days. Over a quarter (**26%**) of security leaders admit their metrics are still at basic or elementary levels of maturity for this group.

It should be remembered that, while metrics should be tailored for different stakeholders, there must be a common thread running throughout or else organisations will suffer from a disconnect between operational and executive decision-making.

SECTION 4:

Metric mayhem

It's clear from the above that trust in metrics data, lack of time and resources, the frequency of requests and knowing which metrics to use are the biggest challenges in developing programmes, with many CISOs admitting they are not yet to reach even intermediate levels of maturity.

Manual, error-prone processes could be to blame for many of these findings. The problem for CISOs is that these deficiencies could have a real impact on the bottom line and/or corporate reputation if stakeholders are provided with inaccurate data, or the wrong metrics altogether.

For example:

Productivity losses for security teams: If there is a security incident, the already time-strapped security teams need to spend a lot more time and effort to investigate the root-cause and then remediate. If the security teams have the capability to continuously monitor and stay on top of control coverage gaps, their productivity can considerably improve, as handling a control incident is less time-consuming and involves less hassle.

Regulatory fines: While GRC teams have tools that manage policies, these tools are ill-equipped to take advantage of existing data from security controls to give metrics that demonstrate that these policies are being followed. Regulators are more lenient with companies that have experienced security breaches if they can demonstrate that they had reasonable security controls in place and were taking due care in protecting their customers' personal data. Also, by being able to align security controls with framework standards, it means that GRC teams can use metrics to demonstrate adherence to regulatory demands.

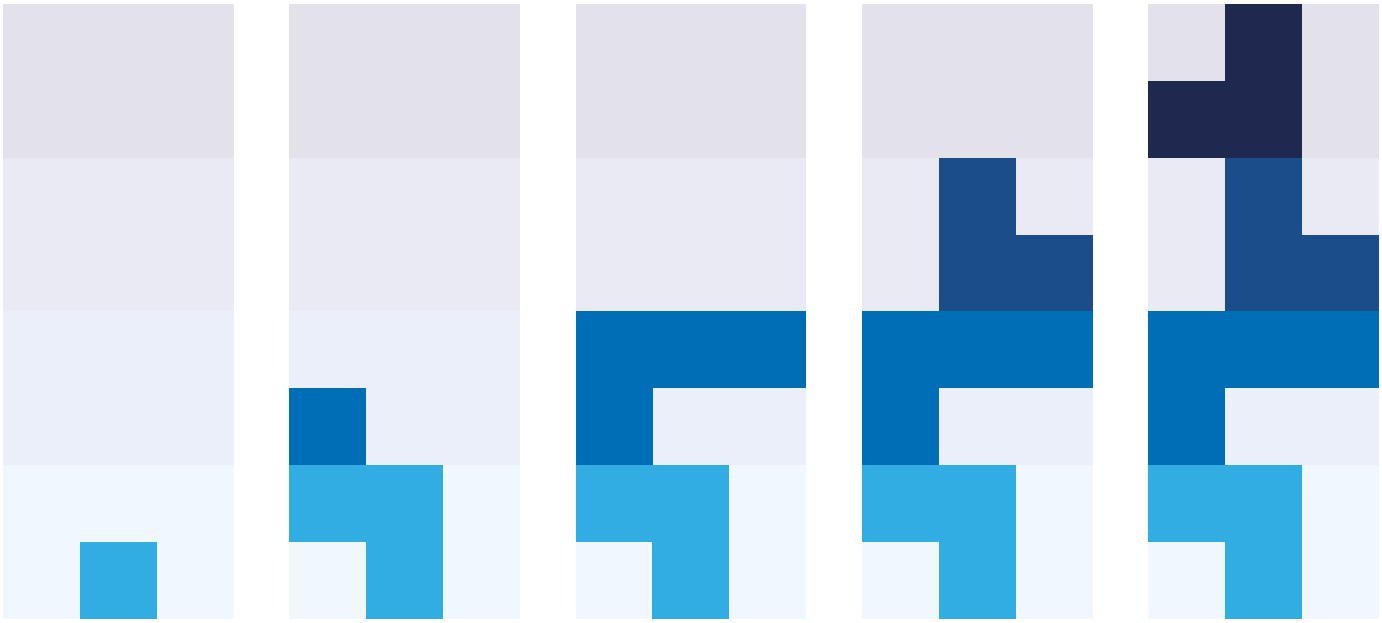
Monetary loss: Regulatory demands are growing in complexity and frequency. Addressing regulators' demands is becoming far more complex for GRC teams, who typically rely on security teams to provide quantitative data to complement the qualitative assessment from GRC tools. If GRC teams get the wrong metrics, their reports to auditors and regulators would be incorrect, potentially leading to severe monetary penalties.

False sense of confidence: If IT teams are using incorrect metrics, or looking at the wrong measurements, they could understate their risk exposure to key stakeholders. That's bad news for the IT function, and for the organisation as a whole.

SECTION 5:

The road to metric maturity

As we've seen, there's a worryingly low level of maturity in many current metrics programmes. We can define the five stages of maturity as follows:



Basic
It's subjective, manual, point-in-time and relies on questionnaires, spreadsheets and consultancies.

Elementary
Still manual, relying on snapshots from data sampling. Exposed to tooling and quality problems.

Intermediate
Features basic automation, data ingestion and storage for simple correlation. But also risks assumption and data problems.

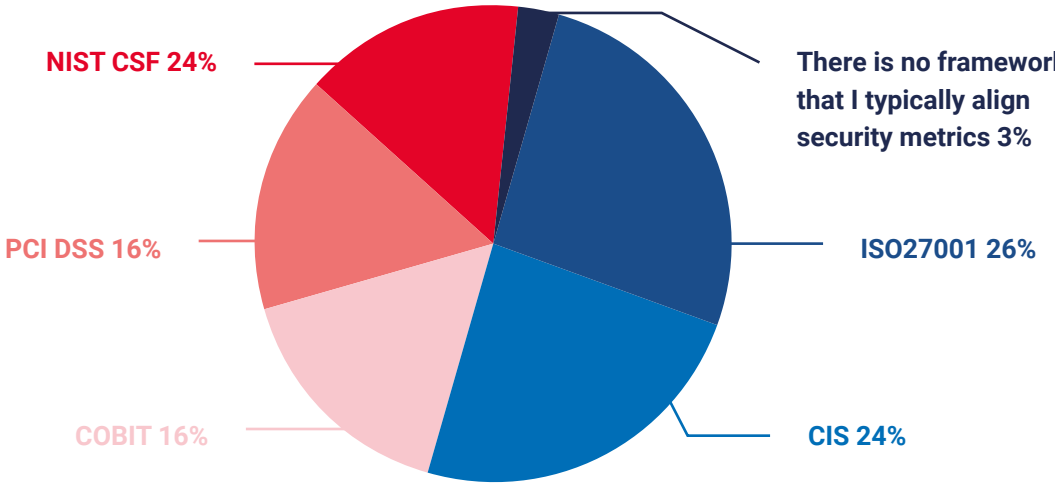
Upper intermediate
Automatic, Continuous Controls Monitoring, providing 360-degree view of IT assets, automated inventory, knowledge graph and business perspectives in a multi-framework approach.

Advanced
Predictive, automated Continuous Controls Monitoring. This approach is able to conduct future extrapolation, predict control failures and take automated action.

SECTION 6:

Getting it right

What frameworks do you typically align security metrics with?



It's good to see that CISOs in financial organisations have set themselves ambitious targets for where they want their metrics programmes to be in 12 months' time. Around two-thirds (**65%**) or more claim they want to be at upper intermediate or advanced stages for all audiences by next year. But getting there won't be easy.

Many are looking to align with frameworks to help them, with ISO 27001 (**26%**), NIST (**24%**) and CIS (**24%**) being the most popular popular. Many also want to align with COBIT (**16%**) and PCI DSS (**16%**).

However, there are few one-size-fits-all solutions to the challenge of security metrics, so frameworks are more commonly used as a foundation on which to build more customised programmes. Security leaders will need to think carefully about how they present metrics in order to accurately align with the frameworks they've chosen, as some require more granular detail than others. Presentation is absolutely crucial to the effective communication of risk or security performance.

Any programmes will also need to take account of new regulations coming down the line, many of which will introduce rigorous new requirements. The MAS Cyber Hygiene Notice for financial firms operating in Singapore, for example, demands a continuous 360-degree view of every asset across multiple controls. Higher levels of metrics maturity will become a must to satisfy such requirements.

Regulations such as SHIELD, CCPA and GDPR require organisations to take due care in protecting systems that hold sensitive data such as PII. In order to do that, organisations would have to identify all assets such as devices, applications, people, accounts and databases that host PII and ensure the right controls are deployed and performing well on these assets. Organisations that aren't mature in security metrics maturity would struggle to address requests like these.

The last word

It's clear that financial sector CISOs are using security metrics in ever greater numbers. But in many cases, low maturity programmes based on fallible manual processes create serious challenges in whether the data can be trusted. Meanwhile, high-frequency demands from multiple stakeholders threaten to overwhelm stretched security teams. The financial and reputational impact on organisations could be severe.

This is why it's crucial for financial enterprises to evaluate if security metrics maturity can be levelled up through internal development or through investment in platforms such as Continuous Controls Monitoring (CCM). Utilising a platform like CCM will help security, risk and IT teams to ensure that all controls are fully operational and all assets are protected.

With CCM, data is cleaned, normalised, aggregated, de-duplicated and correlated as part of the entity resolution process, that increases the data integrity. By unifying disparate data, CCM can identify previously unknown or unmanaged assets and control coverage gaps near real-time.

To move up the scale towards Continuous Controls Monitoring, from a less mature security programme to an upper intermediate level, you need to understand how assets map to business-critical processes.

For example, nobody cares about a vulnerability on a Linux server, but everyone cares about a vulnerability in a payments process.

Having this 'business overlay' and context is crucial, but to achieve it, tools will need to be able to point to data or logic that explains what the organisation looks like.

Next, consider how you define and apply your control checks, and whether this should be automated alongside other basic measurements. A high-quality inventory is also crucial to running a mature metrics programme. Consider combining multiple datasets to gain a complete and accurate picture of your assets, and report on what you don't know.

Ultimately, the goal is to reach full automation that moves your programme to continuously monitor controls coverage gaps, in order to reduce the time it takes to remediate. Understanding risks to the mission-critical parts of the business will help security and risk teams prioritise remediation. This kind of insight will be invaluable for those organisations in helping to save on costs, reduce risk, and optimise their limited teams to deal with surges in workload.

Many financial security leaders will need to decide whether their resources are better spent on investing in an external purpose-built Continuous Controls Monitoring platform or building on in-house capabilities. Given the time pressures, staffing constraints and ever-tightening regulatory reporting regime, expert third-party help may well be the preferred way forward.

Methodology

Panaseer commissioned Censuswide to conduct a survey of security decision makers, at managerial level and above (including CISOs and senior security/risk officers), working in financial services companies with 5,000 or more employees in the UK and US. The web-based survey was fielded January 2020 to February 2020 with a sample size of 403 individuals.

About Panaseer

Panaseer is the first Continuous Controls Monitoring platform to give CISOs visibility of all assets, and the confidence that security controls are working effectively. It provides a trusted, unified view across business processes, regions and technology platforms.

Established in 2014 by Nik Whitfield – a cybersecurity thought leader with extensive FinTech experience. Panaseer's clients include the world's largest financial institutions and critical infrastructure enterprises.

We've got you covered

Continuous Controls Monitoring for enterprise security