


What if knowing your company's cyber security status was as easy as checking the weather?



Key takeaways

1. Moving from a periodic, point-in-time cyber maturity approach to a proactive, real-time cyber status creates a raft of organisational and regulatory benefits.
2. Organisations need to maintain a laser focus on investing in areas that maximise cyber risk reduction before worrying about complex, edge-case scenarios.
3. A continuous assurance model underpinned by key data sources and clear, effective visualisation solves the problem of communicating complex cyber security risk to the board, executives and regulators.

A portrait of Simone Constant, ASIC Commissioner, with blonde wavy hair and red lipstick, wearing a grey textured jacket over a white top. The background is dark with vertical light stripes on the right.

"[Board members need] ...curiosity and gumption to make executives prove that they aren't doing a poor job on cyber security. Don't allow yourself to be told but insist on being shown."

Simone Constant | ASIC Commissioner

The Australian Financial Review Cyber Summit, 17 September 2024

What if knowing your company's cyber security status was as easy as checking the weather?

No one walks out of the house assuming the weather's perfect just because the first day of the month was full of sunshine. Instead, each morning we check our weather apps for the temperature and chance of rain and, armed with that information, decide whether to pack an umbrella or a hat and sunscreen.

Checking your weather app is a cinch because a group of dedicated people have invested the time and effort to build systems and data analysis that all comes together as a local forecast. Having your company's cyber security status at your fingertips should be just as easy.

When it comes to the critical issue of protecting crucial company and customer data, however, the large audit firms have convinced many that a periodic 'maturity assessment' report showing an increase to a wholly subjective maturity approach means only clear skies for their client's cyber security status. This type of tick-and-flick approach not only masks the constantly changing cyber risks facing a company, it's an increasingly untenable position for directors and executives in the eyes of Australian regulators.

The need to maintain a constant watch on cyber functions is borne of both increased external threats and a regulatory environment evolving to meet those threats. Major data breaches experienced by significant Australian companies have helped spur legislative efforts that contain either an implicit or an explicit obligation to clearly monitor a business' cyber security posture, and for the underlying measurements to be built from factual, objective data.

The new APRA CPS 230 Operational Risk Management standard, for example, goes beyond previous prudential standards for banks, insurers and superannuation funds, specifying a requirement for boards to maintain an active engagement in operational oversight. ASIC, meanwhile, has noted that directors can be held personally liable for not effectively assuring their cyber control posture and risk profile. Changes to the Federal Security of Critical Infrastructure Act as well as the new Cyber Security Act, only amplify this focus.

At a recent conference, ASIC Commissioner Simone Constant said that board members needed the “Curiosity and gumption to make executives prove that they aren’t doing a poor job on cyber security. Don’t allow yourself to be told but insist on being shown.”

Even without a push from the regulators, improved cyber security visibility is good business. By getting your cyber security in order, you’ll not only reassure key internal and external stakeholders that you’re meeting the required markers, but it will also help to critically analyse your business’s overall cyber security performance and future-proof your operations.



More than security: How improving your cyber reporting also saves money

Many boards don't feel like they are getting useful information about their organisation's cyber function. With cyber risks increasing and regulators seeking a more proactive approach from directors and senior executives, periodic powerpoint slides on your security environment will no longer cut it.

For many large companies that are asking the question "what is our security posture?", the answer often comes via an audit from a large accounting firm. These audits invariably provide a maturity model-based score out of five, derived from a highly-subjective review of operational processes. There is also a clear threat to the integrity of this process because it's in everyone's interest to say that security is improving while the investment in those audits continues to flow.

This approach is fading fast. For board members and executives, demonstrating active monitoring and management of cyber security risks requires real-time or near real-time visibility of cyber security operations.

Boards also need confidence that the millions of dollars being torched on security programs are actually making a difference.

It's not just directors who are increasingly under the microscope. Everyone from CROs, CIOs, CISOs to senior executives, particularly in the security business, as well as risk and audit, are under more pressure than ever to maintain a close watch on their cyber security functions.

Point-in-time audits are also problematic because they are essentially reactive in nature. When a cyber incident occurs, executives without real-time reporting are typically left scrambling to plug the identified risk. If companies invest in and maintain an approach that measures risk and control effectiveness from key data points over time, companies can constantly track their risk and security control posture performance trends, in turn building a more proactive mindset.

Business leaders need to understand that this is more than a simple issue of compliance. When organisations spend millions, sometimes tens of millions, of dollars annually on cyber security, it is simply untenable to rely on subjective assessments of 'maturity' as the benchmark for achievement.

Sweat the simple stuff: Maximising impact by better understanding risk

It's also important to remember that cyber security isn't just about dealing with complex, edge-case scenarios. Regulators want organisations to mitigate known risks, particularly those being actively exploited by attackers or that have caused known losses in the past.

Boards and executives responsible for the cyber security of an organisation can be easily swept up in the notion they need to prioritise issues with nightmarish names such as 'quantum cryptography rolling to post-quantum algorithms' or 'nation-state hackers using zero day attacks deep in the supply chain'.

These issues are not the big part of the bell curve. The majority of breaches are financially motivated, opportunistic and designed to take advantage of weaknesses that are readily exploitable and, therefore, readily avoidable.

It means that organisations need to maintain a laser focus on investing in areas that have the greatest impact on 'buying down' the overall risk they face.

The Essential Eight, a cyber mitigation checklist developed by the Australian Signals Directorate, is a valuable backbone for such a model: critical patches, hardening internet facing systems, network device configuration and currency, ubiquitous multi-factor authentication and so on.

The beauty of the Essential Eight is that with the right investment in technology and process, every one of the strategies can be monitored in real-time or near real-time. This allows an organisation to have comprehensive visibility of its security standing in a way that genuinely reflects the cyber threats it faces.


You can't manage what you can't measure

The problem with cyber security in most organisations, particularly large, complex organisations, is not that they are missing security controls across their entire business. Instead, it's understanding the gaps and inconsistencies. What aggregates to a maturity level of "3" at a whole-of-organisation level, could easily range from a "5" in small highly functioning teams, through to a "0" in a business acquisition that hasn't yet been integrated.

Moreover, data is often fragmented or simply not available, and it's generally not presented with business context. People are connected to devices, devices and people, in turn, are generally connected to business units, and sometimes to geographic locations. This context, however, is often absent from the dashboards native to security platforms as it requires ingesting information crossing IT, business operations and HR.

A continuous assurance model that categorises data by business unit, by geography, by team or by location, means visibility and individual empowerment is increased on every line. The model also allows the board to see at any moment how their cyber security is functioning and have confidence that they are viewing objective, un-manipulated data. Direct reports to the board, meanwhile, can not only see how their area is performing but what they can do to ensure that there's ongoing regulatory compliance and that the right security protocols are in place.

Heavily-regulated clients can also spend large sums on their risk assurance uplift and cyber security programs, without an effective way of measuring the return on that investment. While taking a bespoke approach may be more expensive in the short-term, a key advantage of continuous assurance is that it gives companies and boards the ability to quickly and clearly draw data-driven conclusions about the efficacy of that spend.



How to have faith in your organisation's cyber maturity

If a board doesn't have a strong number of cyber security experts, how can the board ensure that they are seeing the complete picture of their organisation's risk profile?

Active engagement is key, and boards need to consider two complementary and interdependent principles when understanding their cyber status: structure and completeness.

Structure simply refers to ensuring that there is alignment with industry standards and norms, while completeness refers to the need to ensure reporting does not just include a subjective "maturity" score but that there is an objective "completeness" rating.

Without structure or completeness, there's a strong risk that boards will fall into a sense of false comfort that comes from semi-regular reports showing a maturity rating of 3 or 4, oblivious to the potential scenario that part of the business is completely removed from all the processes covered in that score.

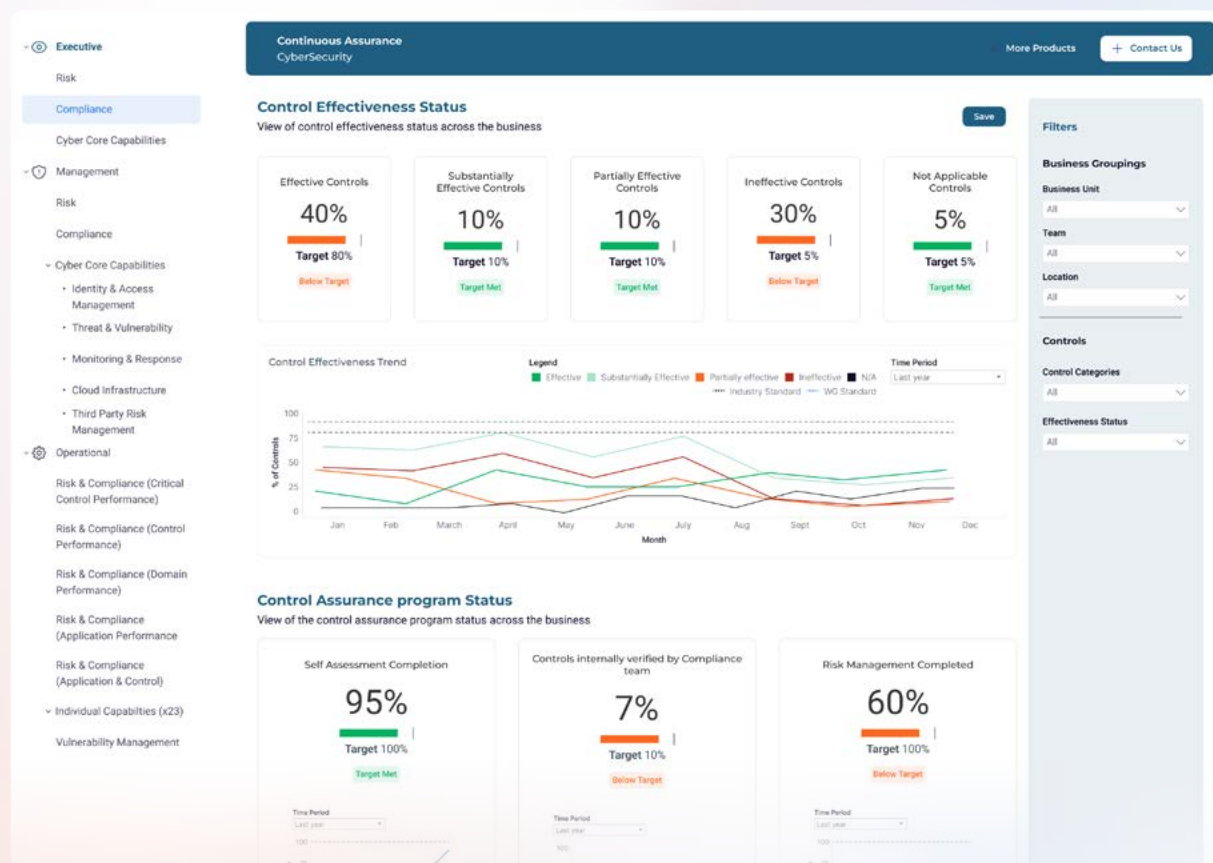
Boards today can overcome these problems by adopting a twin-track approach, consisting of continuous assurance and enterprise reporting:

Continuous assurance

Rather than a periodic, six monthly review, organisations implement systems that are automated, engineering-led, and that monitor and control the cyber security environment on an ongoing basis.

Enterprise reporting

How the data from a continuous assurance program is exposed and communicated effectively to the board and senior executives.



Example of an enterprise report (above)

Much of the problem being solved by such an approach is not, in fact, a 'cyber security' problem. Rather, it's a data problem as well as a visualisation problem.

Cyber security professionals are on the whole incredible at what they do, but their skill sets don't usually extend to being masters of communication. This is, however, something that professional communicators in a digital team are able to do.

Having a cyber partner, such as Mantel Group, that has deep expertise and a track record of bringing the cyber arm of the business together with the digital communication arm, is the key to unlocking true reporting excellence via real-time dashboards.

Continuous assurance with enterprise reporting solves the problem of making cyber security data more usable from the perspective of the executives who are consuming it. It also increases the confidence in the data being presented and allows teams to see how they can contribute to the overall security and compliance of the organisation.

In short, it's being able to check an organisation's cyber security at any moment, not just once a month!

How do you implement continuous assurance?

Every business is different. While there is certainly commonality in some of the platforms, technologies and applications in use, and re-usable components arise from this, continuous assurance is not something that can be bought 'off the shelf'.

Implementing a continuous assurance capability involves a collaborative effort between multiple teams and skill sets: the data team pulls the data together, the cyber team defines the metrics to accurately reflect the security state, and the digital team builds the dashboards and visualisations to bring the resulting models to life.

What actions are required?

1. Before a single piece of code is written, boards need to decide what they want the reporting system to shine a light on. For example, ask yourself, are we meeting our own internal security and compliance standards, or is there a regulatory requirement we need to meet? Are we doing a good job or do we need to know exactly where we're not doing so well? Where do we need additional funding to address any failings?
2. Once the board has clarity on the strategic purpose of the system, it needs to decide how the data is aggregated. Measuring one metric might allow a simplistic single data point for top-line comparisons, but a data-rich, holistic report is a powerful way to see the big picture.
3. Thought should then be given to how attribution will occur, and how the dashboard will be broken down by individual business units, departments, applications, application criticality and so on.

Bringing the data together

Enter the data team. After the parameters of the assurance model have been set, the job of collating, analysing and visualising this data begins. Here is an indicative example of how the Mantel Group team would build a dashboard for real-time cyber analysis.

- ✓ Organise source data from individual PCs, anti-malware software, endpoint controls, network controls to view security controls by cyber, data, digital and cloud.
- ✓ Move from manual analysis to automated analysis.
- ✓ Create a dashboard carrying all key information, including automatically generated security score. This score can be viewed in real time as well as compared historically.
- ✓ If, for example, cyber security is worse than it was six months ago or six days ago, it will be obvious.
- ✓ Option to introduce automation and leverage Gen AI to review and analyse self-assessment reports at scale.
- ✓ Sourcing data with a real-time or a near real time basis means you can drill down and see where the actual problem is.
- ✓ No subjective input from someone tasked with updating slides once every twelve months.
- ✓ A continuous assurance model also gives genuine granularity, allows the board and management to view security outcomes at a business unit level, at a system level.

Let's connect

**Start a conversation about
using technology to impact
organisations in positive ways.**

Contact us