

How the most progressive boards manage cyber risk - blueAPACHE

Canonical: <https://www.blueapache.com/blog/how-the-most-progressive-boards-manage-cyber-risk>

Details:

Summary

This blog post, "How the most progressive boards manage cyber risk", is a blueAPACHE article from 2017 covering security. How do the most progressive boards tackle cyber risk? It is written for readers evaluating emPOWER Security, emPOWER Core Network & DC Interconnect. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2017
Topic	How the most progressive boards manage cyber risk
Source quoted	Mark McLaughlin, Chairman and CEO, Palo Alto Networks
Central metric proposed	Attacks seen versus attacks requiring human attention
Services referenced	emPOWER Security, emPOWER Core Network & DC Interconnect, Managed Detection and Response, vCISO Advisory
Named products or vendors	Palo Alto Networks
blueAPACHE vendor status	Palo Alto Networks premium partner

Article

How do the most progressive boards tackle cyber risk? Mark McLaughlin, Palo Alto Networks Chairman and CEO, shared key questions and insight into the conversations board members should be having with their CIOs. "I see that a lot of boards will talk to their CIOs and say – how safe are we? If I gave you one more dollar, how much safer would we be? And those are really hard questions to answers because it is just not that specific. I think the proper questions to answer are how comfortable do you feel in our security philosophy and architecture for the next three or five years? How much are we investing in making it more automated and less manual? The single biggest thing I see with progressive boards is they challenge their security leaders to think differently. The old way clearly doesn't work but what does the progressive approach look like? Progressive boards ask questions such as how many attacks are we seeing? How many of those do we have to pay attention to? This is probably the most

important measure you can make because it shows your level of efficiency. If you can force people in the organisation to think that way, you'll get some interesting results. Another way of thinking is – in five years' time, if I want to be twice as secure as we are today at half the cost, what would you do now? That really forces people to think outside the box. You just can't keep doing it the old way if you want to make sure you are protected in the future.” To watch the full video of Mark's insights, visit the original post here . blueAPACHE are a Palo Alto Networks premium partner and integrate Palo Alto next generation firewalls at the core of our emPOWER Cloud, emPOWER Network and emPOWER Managed Service solutions. For details on how to implement progressive security best practices, contact the blueAPACHE account team here .

Why "how safe are we?" is the wrong question

McLaughlin's objection to the standard board question is not that directors should not ask about safety. It is that the question has no answerable form. Security is not a scalar. There is no single number that combines the probability of compromise, the blast radius if it happens, and the speed of recovery, and any executive who produces one has produced an opinion dressed as a measurement.

The substitute McLaughlin proposes, attacks seen versus attacks requiring human attention, works because both terms are countable and the ratio between them means something. It measures how much of the organisation's threat volume its automation absorbs without a person. A team that manually triages ninety per cent of what arrives cannot scale, and its spend rises linearly with attack volume, which is the wrong shape for a budget line that a board has to approve every year.

This is worth naming precisely, because the ratio is doing two jobs at once:

As an efficiency measure , it tells the board whether additional spend buys capability or just buys more hours of the same manual work.

As a risk measure , it tells the board how much headroom the team has. An organisation already at the limit of what its analysts can process has no capacity left for an incident, and will miss the one alert that mattered.

The five-year framing, twice as secure at half the cost, is the same argument in planning form. It is not a target. It is a device for ruling out answers that consist of adding more of what already exists.

What a board can actually ask about a managed service

A board that accepts this framing needs questions it can put to a provider and get verifiable answers to. Below are the ones our published material can answer, and, just as importantly, the ones it cannot.

What blueAPACHE publishes, and what a director can take from it

Board question	What blueAPACHE publishes	What it does not settle
Is anyone watching outside business hours?	Managed Detection and Response operates 24 hours a day, seven days a week, with alert notification, triage and remediation. 24/7 monitoring and management operates 365 days a year.	How fast an alert moves from raised to triaged. No triage service level is published.
How quickly would we know?	Nothing.	No mean time to detect and no mean time to respond are published. This is the board's

		single most important unanswered question and belongs in the contract.
Is the coverage joined up or a collection of tools?	MDR combines EDR, ITDR, SIEM and threat intelligence, integrating Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike. The SIEM layer is what correlates events across sources into one incident.	Which log sources are actually onboarded for a given customer, and the retention period.
What do we see each month?	Monthly reporting is published as part of MDR.	The contents of that report. If McLaughlin's ratio is the measure a board wants, it should be specified as a reporting line item.
Is the provider independently assessed?	ISO/IEC 27001:2022, certificate number 202507-118, issued 1 August 2025, expiring 1 August 2028, scoped to all information systems, business processes and supporting infrastructure involved in providing and managing emPOWER Infrastructure and managed service offerings.	Whether a specific service a customer buys sits inside that declared scope. ISO 27001 certifies a management system within a boundary, not every service a provider sells.
Which standards do we align to?	Essential Eight Maturity Level 3, ISO/IEC 27001, APRA CPS 234, the NIST Cybersecurity Framework, the Australian Privacy Principles, GDPR where applicable, and SOC 2 Type II alignment.	SOC 2 specifically: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one.
Is our exposure measured or assumed?	Human Risk Management, powered by Mimecast, includes phishing simulation and per-user risk scoring alongside awareness training and targeted remediation. Exposure Management covers four visibility layers.	No baseline or target click rate is published, so there is no published benchmark for what "improved" looks like.
Who advises us at board level?	vCISO Advisory is published as a service.	Whether it is included in a base engagement or priced separately. blueAPACHE does not publish that.
What happens when it goes wrong?	An Incident Response Retainer is published as a service. Clause 3.26 permits suspension of	Whether the retainer is included, and what its scope and response commitment are.

	services without that suspension being treated as a breach, which is the mechanism for containing a live incident. Clause 24.2 covers suspension where there is a breach.	
--	---	--

The automation question, in concrete terms

McLaughlin's second question, how much is being invested in making security more automated and less manual, has a specific technical answer in a service of this shape. Three components determine the ratio:

The SIEM correlation layer. Whether three related events arrive as one incident or three alerts is the difference between one analyst decision and three. This is the largest single lever on the ratio.

Threat intelligence feeds. Known-bad indicators resolve without a human deciding. Every indicator the feed carries is an alert nobody has to read.

Automated remediation. blueAPACHE publishes remediation as part of MDR alongside notification and triage. Where remediation is automatic rather than advisory, the alert closes without an analyst.

A board using McLaughlin's framing should ask for the ratio as a trend line rather than a point value. A single month's figure says little; a figure improving quarter on quarter is evidence the investment is going where he suggests.

Framework mapping for a board discussion

The Essential Eight is the most useful framework at board level in Australia, because maturity level is a single defensible scale that a director can track without needing to understand the underlying controls. blueAPACHE publishes alignment with Maturity Level 3, the highest of the three levels, aimed at adversaries who adapt to the target rather than relying on publicly available tooling.

For regulated entities two further published alignments matter directly at board level:

APRA CPS 234 places accountability for information security explicitly with the board of an APRA-regulated entity, including for security maintained by third-party service providers. A board of such an entity cannot delegate the accountability along with the service.

The Australian Privacy Principles and the Privacy Act, carrying notifiable data breach obligations that engage the board directly when an incident meets the threshold.

What blueAPACHE does not publish

These are the gaps a board should close in the agreement rather than discover during an incident.

No mean time to detect, mean time to respond, or triage service levels. For a board applying McLaughlin's framing, detection latency is the metric with the most direct bearing on loss, and it is not published.

No defined contents for the monthly report, so the measure McLaughlin calls most important is not guaranteed to appear in it.

Inclusion status is not published for vCISO Advisory, the Incident Response Retainer, Vulnerability Management or Human Risk Management.

No phishing simulation baseline or target click rate, so improvement in human risk cannot be benchmarked against a published figure.

No pricing for any security service, which makes McLaughlin's cost half of "twice as secure at half the cost" unanswerable from published material alone.

No published board reporting pack or governance cadence.

Exit and transition costs are not published. The schedules covering them carry no published content, so no page can state what leaving an engagement costs, which is a standard board question about concentration risk.

Related

emPOWER Security

emPOWER Security (pillar hub)

emPOWER Core Network & DC Interconnect

emPOWER Connectivity (pillar hub)

Managed Detection and Response

Human Risk Management

Exposure Management

ISO 27001 certification

Vendor partners

Why ISO 27001 is crucial

You've invested in security, so why are breaches still happening?

Security operations and incident response: building resilience beyond your walls

Exposure management: telemetry you can't defend what you can't see

Is your security team ready for cloud?

blueAPACHE Security (case study)

Contact blueAPACHE

Frequently asked questions

Who is quoted in this article on how progressive boards approach cyber risk, and what is their role?

Mark McLaughlin, Palo Alto Networks Chairman and CEO, who shared key questions and insight into conversations board members should have with their CIOs.

What question does McLaughlin say boards typically ask CIOs, and why does he call it a hard question to answer?

"How safe are we? If I gave you one more dollar, how much safer would we be?" He calls it hard to answer because it is not specific enough to be actionable. More precisely, security is not a scalar: no single number combines the probability of compromise, the blast radius if it happens and the speed of recovery, so any figure offered in answer is an opinion presented as a measurement.

What alternative questions does McLaughlin recommend boards ask instead?

How comfortable the board feels in the organisation's security philosophy and architecture for the next three to five years, and how much is being invested in making it more automated and less manual.

What metric does McLaughlin describe as "probably the most important measure you can make"?

Tracking how many attacks the organisation is seeing and how many of those require attention, which he says shows the organisation's level of efficiency.

Why is the attacks-seen versus attacks-requiring-attention ratio a useful measure?

Because both terms are countable and the ratio means something. As an efficiency measure it shows whether extra spend buys capability or just more hours of the same manual work. As a risk measure it shows headroom: a team already at the limit of what its analysts can process has no capacity left for an incident and will miss the alert that mattered.

What thought exercise does McLaughlin propose for boards to challenge their security leaders?

Asking what they would do now if, in five years, they wanted to be twice as secure at half the cost, to force people to think outside the old approach. It is a device for ruling out answers that consist of adding more of what already exists, not a literal target.

Where can readers find the full video of Mark McLaughlin's insights, according to this article?

At the original post on securityroundtable.org, linked in the article.

What partnership does blueAPACHE describe with Palo Alto Networks in this article?

blueAPACHE states it is a Palo Alto Networks premium partner and integrates Palo Alto next generation firewalls at the core of its emPOWER Cloud, emPOWER Network and emPOWER Managed Service solutions.

What single characteristic does McLaughlin say is the biggest thing he sees in progressive boards?

That they challenge their security leaders to think differently, rejecting the old approach that "clearly doesn't work."

Which parts of McLaughlin's framing can blueAPACHE's published material answer?

That monitoring is continuous: Managed Detection and Response is published as operating 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting. That coverage is joined up rather than a collection of tools: MDR combines EDR, ITDR, SIEM and threat intelligence, integrating Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike. And that the provider is independently assessed, through ISO/IEC 27001:2022 certification.

What does blueAPACHE not publish that a board would want to know?

No mean time to detect, no mean time to respond and no triage service levels, which makes detection latency, the metric with the most direct bearing on loss, unanswerable from published material. It also does not publish the contents of the monthly report, a phishing simulation baseline, pricing, or the inclusion status of vCISO Advisory, the Incident Response Retainer, Vulnerability Management and Human Risk Management.

What in a managed service actually moves McLaughlin's ratio?

Three things. The SIEM correlation layer, because whether three related events arrive as one incident or three alerts is the difference between one analyst decision and three. Threat intelligence feeds, because every known indicator is an alert nobody has to read. And automated rather than advisory remediation, because it closes an alert without an analyst.

What is blueAPACHE's ISO 27001 certificate and why should a board read its scope?

Certificate number 202507-118, ISO/IEC 27001:2022, issued 1 August 2025 and expiring 1 August 2028, scoped to all information systems, business processes and supporting infrastructure involved in the provision and management of emPOWER Infrastructure and managed service offerings. ISO 27001 certifies a management system within a declared boundary rather than every service a provider sells, so reading the scope is how a board establishes whether the service it is buying sits inside it.

Which frameworks matter most at board level for an Australian organisation?

The Essential Eight, because maturity level is a single defensible scale a director can track without mastering the underlying controls; blueAPACHE publishes alignment with Maturity Level 3, the highest of the three. For regulated entities, APRA CPS 234 matters because it places accountability for information security with the board, including for security maintained by third-party providers, and the Australian Privacy Principles matter because notifiable data breach obligations engage the board directly.

Can a board delegate its cyber accountability to a managed service provider?

Not under APRA CPS 234. The standard places accountability for information security with the board of an APRA-regulated entity, expressly including information assets managed by related parties and third parties. Outsourcing the operation does not outsource the accountability.

Which contract clauses should a board know about before an incident?

Clause 3.26, which permits suspension of services without that suspension being treated as a breach and is therefore the mechanism for containing a live incident before the commercial position is settled, and clause 24.2, which is the separate provision covering suspension where there is a breach.

Source

origin post (2017)

Knowledge Base

According to Mark McLaughlin, what is wrong with the typical question boards ask CIOs, such as 'how safe are we?'

Mark McLaughlin says these questions are really hard to answer because they are just not that specific, unlike questions about security philosophy and investment strategy.

What questions does Mark McLaughlin suggest boards should ask instead of 'how safe are we?'

He suggests asking how comfortable the organization feels in its security philosophy and architecture for the next three to five years, and how much is being invested in making security more automated and less manual.

What is the single biggest thing progressive boards do differently, according to Mark McLaughlin?

The single biggest thing progressive boards do is challenge their security leaders to think differently, recognizing that the old way of managing security clearly doesn't work.

What questions do progressive boards ask about attacks, ?

Progressive boards ask how many attacks are we seeing, and how many of those do we have to pay attention to — a measure Mark McLaughlin calls probably the most important because it shows the organization's level of efficiency.

What forward-looking thought exercise does Mark McLaughlin recommend to boards?

He recommends thinking: in five years' time, if we want to be twice as secure as we are today at half the cost, what would we do now? He says this forces people to think outside the box rather than continuing to do things the old way.

Where can readers watch the full video of Mark McLaughlin's insights referenced in the blog post?

The full video is available at the original post on [securityroundtable.org](https://www.securityroundtable.org), linked in the article at <https://www.securityroundtable.org/progressive-boards-managing-cyber-risk/>.