

Security Simplified: A Pragmatic Approach - blueAPACHE

Canonical: <https://www.blueapache.com/blog/security-simplified-a-pragmatic-approach>

Details:

Originally published 26 July 2017. The event account below is historical; the practical guidance that follows is an updated companion to it.

In July 2017, blueAPACHE hosted an Insight Event luncheon in Melbourne. The original article described these events as intimate discussions limited to a single table, giving attendees an opportunity to speak with an industry expert about organisational challenges. The 2017 article identified Bill Robson as blueAPACHE's Security Practice Lead and described more than 20 years of information-security experience, including consulting and penetration-testing roles with PricewaterhouseCoopers and Deloitte. These role and experience details are historical. The discussion, over some really good wine and steak, focussed on how technology threats can translate into business risks and a pragmatic way for organisations to assess and combat that risk. The article described organisations' concerns about security complexity, cost and keeping pace with threats.

"What I've observed is that often there is a disconnect between technologists and key decision makers within organisations", said Bill. "While security experts tend to worry about the nitty-gritty of day to day running of their networks and systems, they often miss the commercial reality of doing business. The answer lies in using the language of risk to communicate."

Key aspects of Bill's pragmatic approach to security include:

Information security is not the sole responsibility of the IT team. In order for your security measures to be successful, every business unit needs to be involved in the conversation regarding what constitutes a risk and the cost of combating it.

There is no need to reinvent the wheel. Identify and utilise industry standard compliance tools and best practises.

Use an information security risk register to drive the security agenda and make use of smart tools, not spreadsheets, to manage your risk register.

The original article thanked attendees and invited expressions of interest in future Insight Events. For current events or security services, contact our team .

Unpacking the three recommendations

The following suggestions build on the article's three themes. They are practical guidance, not additional quotations or a claim about the detailed methodology presented at the 2017 event.

"Information security is not the sole responsibility of the IT team"

Bring technical, business and relevant legal or compliance expertise into risk assessment. Technical teams can explain systems and exposure; business stakeholders can help assess operational impact, data value and acceptable disruption. Agree decision-making responsibilities rather than assuming one function has all the necessary context.

A useful approach is to identify an owner for important assets and jointly review classification, acceptable disruption and recovery needs. Define recovery time and recovery point objectives in the

recovery design, check their feasibility and agree who approves them. This is suggested practice, not a universal three-signature requirement.

For entities within its scope, APRA CPS 234 places ultimate information-security responsibility with the Board and requires roles to be defined across management and other responsible functions. It also requires asset classification by criticality and sensitivity. Separately, the Australian Privacy Principles govern relevant handling of personal information by APP entities. Determine which obligations apply to your organisation. CPS 234 commenced in 2019; it is later context, not a standard named in this 2017 account.

"There is no need to reinvent the wheel"

The original article recommends industry standards without naming the following frameworks. These are examples to assess for present-day requirements; use the current version and applicable scope:

Framework	What it is for
ASD Essential Eight	Eight mitigation strategies supported by a maturity model with four levels, Zero through Three. Select a target appropriate to the environment and consider additional controls where needed. ASD model
ISO/IEC 27001:2022	Requirements for establishing, implementing, maintaining and improving an information security management system and managing information-security risk. Certification relates to the defined ISMS scope. ISO overview
NIST Cybersecurity Framework 2.0	Organises cybersecurity outcomes across six functions: Govern, Identify, Protect, Detect, Respond and Recover. Version 2.0 was published in 2024. NIST CSF 2.0
APRA CPS 234	Prudential information-security requirements for entities within its scope, including accountability, asset classification, control testing and APRA notification. Check applicability and any adjustments or exclusions. APRA standard
Australian Privacy Principles	Requirements for APP entities concerning personal-information handling, including collection, use, disclosure, security, access and correction. OAIC reference

Our security materials refer to several standards and frameworks. A reference or alignment statement does not itself establish legal compliance, certification, an independent assurance report or the controls included in a customer's service. Request the relevant evidence for the scope you need.

Our brochure states Essential Eight Maturity Level 3 alignment. ASD's model defines levels Zero through Three, and Level Three is not a guarantee against compromise. Our ISO/IEC 27001:2022 certificate 202507-118 is valid from 1 August 2025 to 1 August 2028 for its stated ISMS scope covering emPOWER infrastructure and managed-service operations. Check the certificate and assessment scope against your requirements; these later claims are separate from the 2017 event.

"Use a risk register, and smart tools, not spreadsheets"

Robson recommended smart tools rather than spreadsheets. When choosing a register tool, consider ownership, review dates, change history, links to controls and supporting evidence. Evaluate how the actual tool and process provide these capabilities; the file format alone does not determine collaboration or audit history.

A suggested entry records the asset, owner, threat, likelihood and consequence, treatment decision, residual risk, review date and evidence. Adapt those fields to your methodology and governance needs; they are an illustrative template, not a prescribed format from the original article.

Translating a threat into a business risk

Robson advocated using the language of risk to connect technical and business decisions. The following is one illustrative way to structure that conversation.

A technical finding says: this server is missing a patch for a known remote code execution vulnerability. That statement has no decision in it. Converting it to a business risk means answering four further questions:

What does the server hold or do? Customer records, or the meeting room booking system. This is asset classification, and it comes from the business owner.

What would an attacker be able to do with it? Read, alter, destroy, or move elsewhere from it. This determines whether the consequence is a privacy breach, a financial loss, or an outage.

What would that cost? Regulatory exposure, notification obligations, contractual penalties, lost revenue per hour of downtime, remediation cost.

What does treatment cost, against that? Patching effort, downtime to apply it, compensating controls if it cannot be patched.

These questions can help compare treatment options with business impact, legal obligations and risk appetite. They are not a mandatory sequence or the only basis for a decision. Similar technical findings can warrant different responses when the affected assets and business consequences differ.

Advisory

We publish vCISO Advisory as a service. This is the capability Robson's argument implies: someone who can sit between the technical detail and the board and perform the translation described above.

Assessment

Our portfolio describes Vulnerability Management and Exposure Management capabilities. Discuss the assets, assessment methods and visibility sources included in your service, and how findings will feed the risk register. An external attack-surface assessment provides a view of exposed assets within its scope rather than complete knowledge of everything an attacker could discover.

Ask for any Vulnerability Management inclusion, coverage and reporting to be recorded in the Service Order.

Detection and response

We publish Managed Detection and Response combining EDR, ITDR, SIEM and threat intelligence, operating 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike.

Against the risk register, the monthly report is the natural review input. If the register is to be reviewed rather than written once, something has to trigger the review, and a monthly operational report is the obvious candidate.

The human dimension

Human Risk Management , published as powered by Mimecast, has four components on a prevent, detect, respond and reduce lifecycle: awareness training, phishing simulation, per-user risk scoring and targeted remediation. The risk scoring is what turns "our people are a risk" into a measured, per-user figure that can sit in a register rather than a slide.

Contract terms

When a risk treatment depends on a managed service, review the applicable agreement alongside the incident-response plan. Under General Terms v3.6:

Clause 3.26 addresses specified suspension or cancellation circumstances, including upstream withdrawal or replacement, with notice, mitigation and fee provisions. It is not an incident-containment runbook.

Clause 24.2 sets out blueAPACHE's termination rights, including specified breaches and cure periods after written notice. It is not a general suspension clause.

Record relevant service dependencies and confirm the following with the provider:

Detection and response: agree covered threats, escalation, authorised actions and any response or triage commitments, including how they are measured.

Reporting: agree the MDR report contents and how findings and incidents inform risk review.

Service inclusions: request explicit scope for any vCISO Advisory, Vulnerability Management, Incident Response Retainer or Human Risk Management services you intend to rely on.

Human risk measures: agree the phishing-simulation baseline, target measures, cohort and comparison period rather than assuming a universal benchmark.

Recovery objectives: agree recovery time and recovery point objectives for the covered workloads, along with testing and evidence that the proposed design can meet them.

Risk assessment: agree the methodology, register format, review cadence and approval responsibilities appropriate to your organisation.

How did the 2017 article describe Bill Robson?

The article published on 26 July 2017 identified Bill Robson as blueAPACHE's Security Practice Lead and described more than 20 years in information security, including consulting and penetration-testing roles with PricewaterhouseCoopers and Deloitte. These are historical role and experience details.

How did the article describe blueAPACHE Insight Events?

The 2017 article described intimate luncheon discussions limited to a single table, where attendees could ask an industry expert questions and discuss organisational challenges.

According to Bill Robson, what disconnect often exists within organisations regarding security?

In the 2017 article, Bill Robson described a disconnect between technical security concerns and business decision-making, and advocated using the language of risk to communicate.

What are the key aspects of Bill Robson's pragmatic approach to security?

The 2017 article presents three recommendations: involve business units in conversations about risk and the cost of treatment; use industry standards and practices; and use a risk register supported by smart tools. The article does not name the later framework examples in the companion guidance.

How can someone ask about current blueAPACHE events?

The historical article invited interest in future Insight Events. Use the current contact page at <https://www.blueapache.com/contact> to ask about events and availability.

How can someone learn more about your security offering?

Use the contact page at <https://www.blueapache.com/contact> to discuss current security services and agree the scope relevant to your organisation.