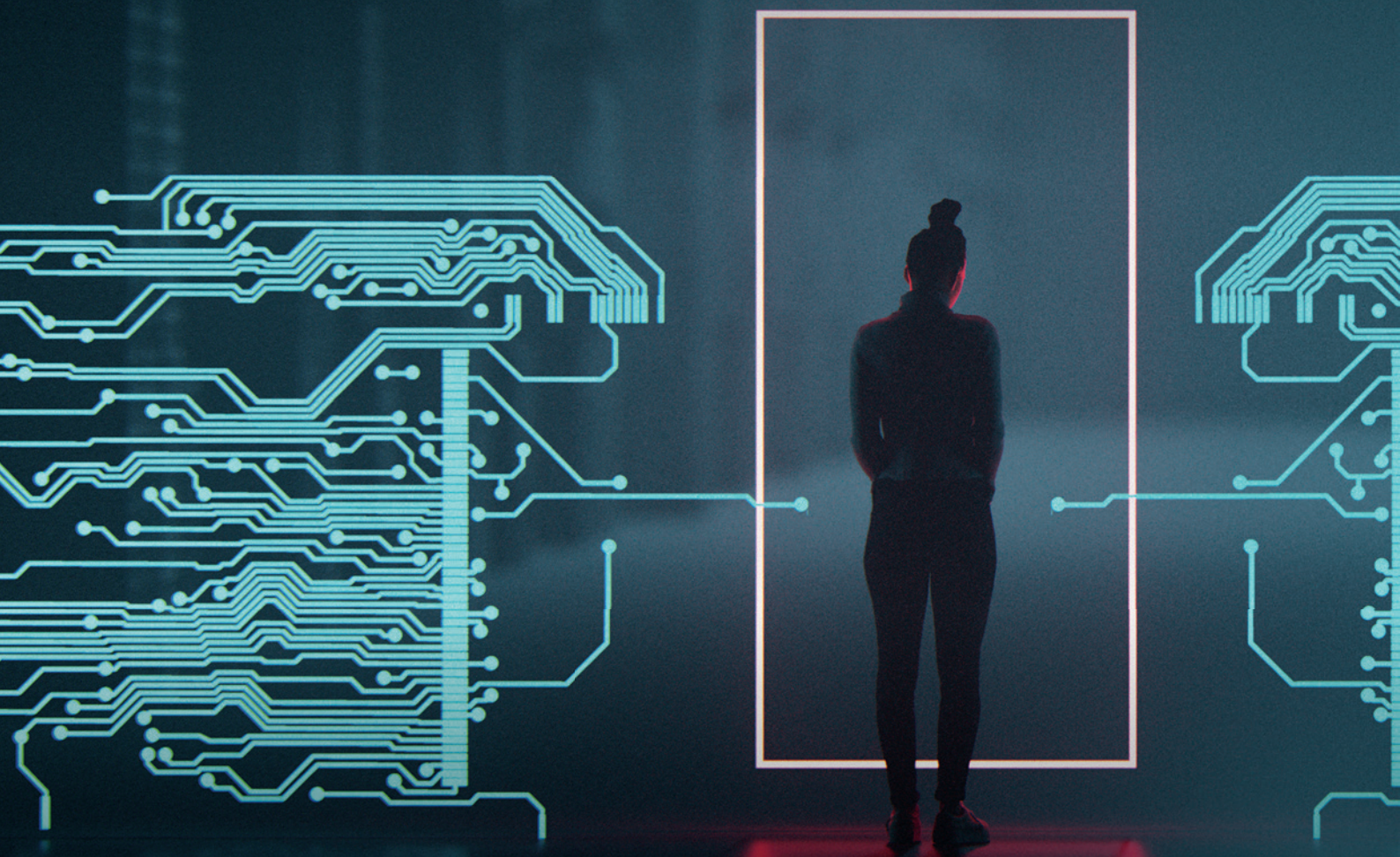
Cyber Today

EDITION 2, 2025

CYBER SECURITY ON A SHOESTRING

WINNING THE CYBER BUDGET – A HALLMARK OF WOMEN IN LEADERSHIP

A DAY IN THE LIFE OF AN SOC MANAGER: PEOPLE, PRESSURE AND PRIORITIES



AISA

SANS

Defend with Confidence in Uncertain Times

Secure your future with elite cyber training from SANS

Strengthen Your Cyber Resilience Limited-Time Offer Now Available

SANS recognises the pressure facing today's cybersecurity teams. In an unpredictable threat landscape, timely and effective training makes the difference between vulnerability and resilience.

To help you stay ahead, we're offering a limited-time promotion on our most in-demand courses, empowering your team with world-class skills and savings of up to **30%.**
Hurry Offer ends 31st December, 2025.

ACT NOW to take advantage of this opportunity and level up your cyber defence.

The Offer

- **Level 300 & 400 courses |** 30% discount (up to $4,005) to the course price
- **Level 500 courses |** 20% discount (up to $2,670) to the course price

This offer is not valid with any other promotions. SANS Voucher customers, get in touch with us to discuss available options

Eligible Australia based Events

- **SANS Spring Sydney**
  22-27 September 2025
- **SANS Brisbane**
  13-18 October 2025
- **SANS Canberra November**
  3-8 November 2025

For more information, email us at **anz@sans.org** **www.sans.org** **+61 2 6174 4581**

PUBLISHED BY :

EXECUTIVE MEDIA
NEW YORK | MELBOURNE | ADELAIDE | AUCKLAND

ABN 30 007 224 204

PO Box 256, North Melbourne, VIC, 3051

Tel: 03 9274 4200
Email: media@executivemedia.com.au
Web: www.executivemedia.com.au

PUBLISHER
David Haratsis
david.haratsis@executivemedia.com.au

EDITOR IN CHIEF
Giulia Heppell
giulia.heppell@executivemedia.com.au

CO-EDITOR
Craig Ford

EDITORIAL ASSISTANTS
Eden Cox and Ruby O'Brien

DESIGN
Sam Garland

PARTNER ORGANISATION
SANS Training Australia

Contents

Foreword

A message from David Willett, Board Member, AISA.

David Willett

Who doesn't love a good story? Ever since the earliest Indigenous cultures, storytelling has been a vital part of society – often seen as a primary means of transmitting knowledge, history and cultural values across generations. It's more than just entertainment; it's a powerful tool for education, preserving oral traditions, and fostering connections to land, community, and heritage.

Fast forward to today, and we share stories through written, visual, and other media. We hover around our televisions to feast our eyes on well-told narratives, we flock to theatres for adventures performed live, and we lose ourselves to plots told through the written word. Naturally, the one thing that makes a story infinitely more compelling is a retelling of true events. Is it any wonder, then, that cyber security professionals are becoming more adept at storytelling? This is the case whether it be to each other, our bosses, stakeholders, peers, or even family and friends. Like many others, cyber security stories come with morals and lessons to be learnt.

Consider the relative freshness of the cyber profession. I remember the glazed-over eyes I got at barbecues when I clumsily tried to explain my line of work, and this was only back in 2019. These days, the mere mention of working in cyber results in people wanting to tell their stories, while also hearing mine – all in the interests of helping each other understand how to live more digitally safe lives. Everyone has seen the headlines, everyone has been impacted and everyone wants to know more.

We also tell stories within cyber teams – about vulnerability, and how the security operations centre analysts translate unpatched software and indicators of compromise into cautionary tales. This helps the CISO craft a story for their executives and boards about how threats, both real and existential, require immediate attention. Without the art of the story, it is just numbers on a page. Who would want to binge watch that?

Then we have the stories we share within our cyber community, propelled by a deep desire to share experiences and learn. Cyber true crime podcasts have become some of the most downloaded on the internet. We tune in every week to hear just how some crafty hackers managed to bring a well-known organisation or government to its knees. Did they or did they not pay the ransom? We cannot wait to find out, while also hoping to learn from the wisdom gained through others' misfortune.

It is no wonder that CISOs, incident responders, and white hat hackers are the superstars of our conferences, especially if they lived through a real breach. We gather around their podiums like a camp fire to hear their harrowing tales. They share anecdotes to enshrine their stories in the history of our cyber culture, so that we can learn and grow, like people have done since the dawn of time.

The stories we tell in cyber bolster Australia's digital resilience. They are not just about horrific breaches, either; however, they can be the most interesting, at times. As you browse the articles in this edition of *Cyber Today*, I encourage you to absorb the fascinating stories from our contributors. Every writer brings their unique experiences and a desire to share their insights with you. The stories they tell range from business-aligned cyber security and invisible supply chain dependencies, to human leadership and empathy, psychological warfare, and the democratisation of cyber resilience. Taking in the morals of each story will hopefully advance your knowledge and approach to your career. You may even be compelled to tell a story of your own.

The Australian Information Security Association offers numerous opportunities for members to share stories. You can contribute to a publication like this one, speak at CyberCon, at SEC days, or a branch meeting, or you can even come and chat with me on our official podcast, *Cyber Voices*. I encourage you to embrace abstraction, storytelling, and inclusive leadership as tools for navigating complexity and building resilient systems.

Finally, I would like to echo a sentiment from 'Ghosts in the machine', one of the articles you'll find within: 'In the mythology of cyber conflict, the side with the better story often wins.'

Beyond the boundary: abstracting cyber security supply chain risk as an nth-order Markov problem

BY DR SRIRAM RAGHAVAN

Abstracting cyber security supply chain risk as an nth-order Markov problem offers a structured and potentially powerful way of mitigating threats.

The expanding digital interconnectedness of modern business has woven a complex web of dependencies that stretch far beyond the traditional enterprise perimeter. While organisations have made significant strides in securing their internal infrastructures, the escalating threat landscape is increasingly focused on exploiting vulnerabilities in the supply chain – the intricate network of third, fourth, and even nth parties upon which businesses rely.

Managing this risk is not merely a technical challenge; it is a strategic imperative with profound implications for business continuity, financial stability and regulatory compliance. This article explores the potential for abstracting and modelling this complex challenge, particularly concerning the myriad software dependencies that underpin modern systems, through the lens of an nth-order Markov problem. While fraught with inherent difficulties, this approach offers a structured methodology for understanding, quantifying and ultimately mitigating a risk that often feels boundless.

The tangled web: understanding cyber security supply chain risk

At its core, cyber security supply chain risk is the potential for harm to an organisation's information systems or data that arises from vulnerabilities or compromises within its vendors, partners, suppliers, or the products and services they provide. This extends beyond the initial provider (the 'third party') to their providers ('fourth parties'), and potentially many layers deeper.

Consider a typical software product, especially a sophisticated cyber security platform. It is rarely built entirely from scratch. It incorporates commercial off-the-shelf components, integrates with third-party services (like cloud providers, identity platforms and threat intelligence feeds), and heavily relies on a vast ecosystem of open-source software libraries and modules. Each of these dependencies introduces a potential attack vector. A vulnerability in a widely used open-source cryptographic library, a misconfiguration in a cloud service provider, or a breach at a managed service provider can have a cascading effect, directly impacting the security posture of the relying organisation.

For senior executives, this translates to potential business disruption, loss of customer trust, reputational damage, and significant financial costs associated with incident response, remediation, and potential litigation or regulatory fines. For risk and insurance professionals, it represents a burgeoning area of exposure that is difficult to assess and underwrite. For security and technical architects, it's a constant battle for visibility and control over components they did not build and do not directly manage.

The illusion of control: crossing organisational boundaries

One of the most significant challenges in managing supply chain risk emerges precisely when we cross organisational boundaries. Traditional risk management frameworks often rely heavily on contractual agreements, security questionnaires, and service-level agreements (SLAs). These mechanisms define expected security controls, response times for incidents and other crucial requirements; however, the reality on the ground is often far more complex, including:

- **Information asymmetry:** The relying organisation is fundamentally dependent on the third party to provide accurate and timely information about their security posture, and any incidents. There is limited capability for independent, continuous verification.
- **SLAs as point-in-time assurances:** While legally binding, SLAs primarily represent a point-in-time agreement or a set of static requirements. They offer little insight into the dynamic evolution of a third party's security environment, their ongoing vigilance, their response to emerging threats, or the security practices of their suppliers (the fourth parties).
- **The 'Black Box' problem:** For many services and software components, the internal workings of the third party's security operations, development practices, and dependency management remain a black box. Relying solely on contractual obligations feels increasingly insufficient when faced with sophisticated, rapidly evolving threats.
- **Software supply chain opacity:** This problem is acutely magnified when dealing with software dependencies, particularly open-source components.

- **Unknown ownership:** Identifying the true maintainers or contributors to a specific open-source module used deep within a dependency chain can be difficult or impossible.
- **Transient parties:** Open-source projects can be abandoned, maintainers can change and the community supporting them can fluctuate.
- **Licence as the sole link:** Often, the only formal relationship is the licence agreement (like Apache, MIT and GPL), which grants usage rights but provides no ongoing assurance of security maintenance, vulnerability patching, or even continued project existence. A licence is a legal document, not a dynamic security monitoring feed.
- **The fourth party and beyond problem:** Tracing the dependencies of your dependencies – the libraries used by the libraries your vendor uses, or the cloud provider used by your SaaS provider – quickly becomes a combinatorial explosion. Each layer adds complexity, reduces visibility, and introduces new potential points of failure, making the challenge feel endless.

This lack of continuous visibility and verifiable assurance means that a risk assessment based on an annual questionnaire or an SLA document provides only a static, potentially misleading snapshot of a highly dynamic situation. We need a way to model the *evolution* of risk over time, accounting for dependencies and the probabilistic nature of events like vulnerability discoveries, exploits, and patches.

Modelling risk as a dynamic process: introducing Markov chains

Traditional risk assessment often focuses on identifying assets, threats and vulnerabilities, and calculating a static risk score (risk = likelihood × impact). While useful, this doesn't inherently capture the process of risk evolving over time. This is where probabilistic models like Markov chains can offer a valuable perspective.

A Markov chain is a mathematical system that transitions from one state to another based on specific probabilistic rules. A key property of a first-order Markov chain is that the probability of transitioning to the next state depends only on the current state, and not on the sequence of events that preceded it (the 'memoryless' property). Let's imagine a simplified system's security state could be represented by discrete states, such as:

- $\mathbf{S_0}$**:** Secure (no known vulnerabilities or compromises)
- $\mathbf{S_1}$**:** Vulnerable (a known vulnerability exists)
- $\mathbf{S_2}$**:** Compromised (the vulnerability has been exploited)
- $\mathbf{S_3}$**:** Propagating (the compromise is spreading).

A first-order Markov model would define transition probabilities between these states. For example, $P(S_1 \mid S_0)$ would be the probability of transitioning from Secure to Vulnerable in one time step (e.g., due to a new vulnerability discovery), and $P(S_2 \mid S_1)$ would be the probability of moving from Vulnerable to Compromised (e.g., due to an exploit occurring). The state of the system at time t, denoted by a vector $s_t=[P(S_0)_t, P(S_1)_t, P(S_2)_t, P(S_3)_t]$, where each element is the probability of being in that state at time t, can be calculated using the transition matrix T, where $T_{ij} = P(S_j \mid S_i)$:

$$s_{t+1} = s_t T$$

This basic model can represent simple transitions, but supply chain risk is rarely this straightforward. The probability of a third-party software library vulnerability leading to a compromise in your system might not just depend on the library currently having a vulnerability (S_1); it might also depend on:

- whether you failed to patch a previous vulnerability in that library (i.e., your state at $t-1$)
- whether a different, related library from the same vendor or open-source project also had vulnerabilities recently (i.e., the state of a related component at t or $t-1$)
- whether a specific security control failed in the past that would have detected this type of vulnerability (i.e., the state of a control mechanism at $t-k$).

These scenarios introduce memory into the system. The next state depends not just on the current state, but on a sequence of previous states. This requires an nth-order Markov chain, in which the probability of the next state depends on the n most recent states:

$$P(State_{t+1} \mid State_t, State_{t-1}, \ldots, State_{t-n+1})$$

To model this formally, we often redefine the 'state' to encompass the history of the

last n steps. For example, in a second-order chain (n = 2), the states might become (S_i, S_j), representing being in state S_i at time t and S_j at time t-1. The transition then occurs from (S_i, S_j) to (S_k, S_i) with probability $P(S_k \mid S_i, S_j)$. As n increases, the number of possible states explodes combinatorially, making the model significantly more complex.

Abstracting supply chain risk as an nth-order Markov problem

The proposition is to abstract the security posture of a critical part of the supply chain – specifically the interconnected network of software components – as a system evolving through discrete states (S_0, S_1, ... ,S_m) over time. These states represent different levels of risk exposure, from 'components fully compliant and patched' to 'critical vulnerability exploited and propagating'.

The transition probabilities between these states are what an nth-order Markov model attempts to capture. The 'nth order' is crucial because the risk profile isn't just about the *current* known vulnerability; it's influenced by the history of patching, past security incidents with that vendor/project, the age of components, and the cumulative effect of multiple lower-severity issues.

The challenge: defining states and probabilities across boundaries

Applying this theoretical model to the chaotic reality of supply chain risk, especially involving opaque third and fourth parties, and sprawling open-source dependencies, immediately highlights significant challenges:

- **Defining comprehensive states:** What are the relevant states for a software supply chain? It's not just about individual vulnerabilities. States need to capture the aggregation of risk across multiple components, the status of mitigation efforts, and the potential for propagation. Defining a finite, manageable set of states that accurately reflects the complex reality is difficult.
- **Determining transition probabilities:** This is arguably the biggest hurdle. How do you determine the probability that a vulnerability in a fourth-party open-source library (State S_i for that component) will transition to an exploited state (State S_j) that then transitions your system to a compromised state (State S_k), *especially* when the vulnerability disclosure, patching status, and exploitation attempts are largely invisible within the third or fourth party's domain? Relying solely on SLAs doesn't provide the dynamic, probabilistic data needed
- **The nth-order explosion:** As noted, increasing n to capture more history makes the state space and the number of transition probabilities (mn+1) grow exponentially, demanding vast amounts of data for estimation and quickly becoming computationally intractable for large, realistic supply chains. This reinforces the 'never-ending challenge' perception. If we try to model every possible state and every dependency's history, the problem becomes impossible to manage.

Making it tractable: selecting parameters and measurement mechanisms

The key to making this abstraction useful lies entirely in selecting a limited and relevant range of parameters that can serve as proxies for the system's state and significantly influence transition probabilities, rather than modelling the whole risk chain. These parameters must be:

- **Measurable:** The parameters should be quantified, calibrated and measurable, directly or referred.
- **Relatable:** The parameters should correspond to identifiable technical security controls or business/operational factors.
- **Influential:** The parameters should have a demonstrable impact on the likelihood of moving between desired and undesired risk states.

By focusing on these key parameters, we can potentially abstract the system's state and its transitions in a more manageable way. The 'memory' (nth order) is implicitly captured by tracking parameters that reflect historical performance or cumulative risk factors.

Identifying relatable business and technical parameters

Let's consider parameters relevant to the security of third-party software libraries and open-source modules used in a cyber

security platform. These parameters can serve as inputs to estimate transition probabilities between defined states:

Technical parameters

1. **Vulnerability count and severity (VCS):** the number and severity of *known* vulnerabilities in the specific library/module and its direct dependencies. A high VCS increases the probability of transitioning to a 'Vulnerable' state or remaining in one.
2. **Patch velocity (PV):** the average time it takes the vendor or open-source project maintainers to release a patch after a vulnerability is publicly disclosed. Slow PV increases the probability of transitioning from 'Vulnerable' to 'Exploitable' or 'Compromised'.
3. **Component age and maintenance (CAM):** the age of the library/module and the perceived level of active maintenance (e.g., frequency of commits, release cycles, open issue count in open source). Older, less maintained components may have unknown vulnerabilities or slower patch cycles, increasing vulnerability transition probabilities.
4. **Static/dynamic analysis results (SAR):** findings from code analysis tools run against the component or products using it. Poor SAR scores indicate higher likelihood of vulnerabilities, influencing transitions to 'Vulnerable'.
5. **Dependency depth and breadth (DDB):** the number of layers of transitive dependencies and the total count of unique components. Deeper and broader dependencies increase the attack surface and the potential for unknown risks, influencing the probability of unexpected transitions to 'Vulnerable' or 'Compromised'.

Business/operational parameters

1. **Vendor security score/audit results (VSR):** Scores from vendor security questionnaires, independent audits (e.g., SOC 2 Type II), or penetration test results provided by the vendor. A low VSR suggests weaker security practices, increasing the likelihood of the vendor experiencing a compromise that could propagate.
2. **Security incident history (SIH):** the frequency and severity of past security incidents reported by the vendor or related to the open-source project. A history of incidents increases the estimated probability of future incidents and transitions to 'Compromised' states.
3. **Contractual security requirements and enforcement (CSRE):** the stringency of security clauses in contracts/SLAs and the organisation's ability to verify and enforce compliance. Weak CSRE provides less assurance and higher likelihood of adverse state transitions originating from the third party.
4. **Financial viability of vendor (FVV):** the financial health and stability of a commercial vendor. A vendor facing financial distress may reduce investment in security, slow down patching, or even cease operations, increasing the probability of vulnerabilities remaining unaddressed or support disappearing.
5. **Geopolitical risk (GPR):** the political stability and threat landscape in the geographic location(s) where the vendor or open-source contributors are based. High GPR might correlate with increased risk of state-sponsored attacks or supply chain interference, influencing transition probabilities to 'Compromised' or 'Malicious Code Injection' states.

Suitable mechanisms to measure and track

To use these parameters in a probabilistic model, we need mechanisms to measure and track them over time:

- **Automated scanning tools:** software composition analysis (SCA) tools to identify open-source components and known vulnerabilities (VCS, CAM, DDB). Static application security testing (SAST) and dynamic application security testing (DAST) on integrated products (SAR).
- **Threat intelligence feeds:** subscriptions providing timely information on new vulnerabilities (CVEs), exploits, and

incidents related to specific software components or vendors (VCS, PV, SIH).
- **Vendor risk management (VRM) platforms:** tools to manage and score vendor security questionnaires and track audit documentation (VSR, CSRE).
- **Open-source community monitoring:** tools or processes to monitor activity in open-source repositories, track patch releases and observe community health (PV, CAM).
- **Contract management systems:** tracking and reviewing security clauses and performance against SLAs (CSRE).
- **Financial monitoring:** basic financial health checks on critical commercial vendors (FVV).
- **Geopolitical analysis:** incorporating relevant country risk assessments (GPR).

Tracking these parameters over time allows us to estimate the transition probabilities within our simplified Markov model. For example, observing that a vendor with a low VSR score historically takes longer to patch critical vulnerabilities (slow PV) provides data to estimate the probability of transitioning from 'Vulnerable' to 'Exploited' for components from that vendor.

The value of using nth-order Markov equations

Even with the inherent limitations, abstracting supply chain risk using an nth-order Markov framework with selected parameters offers significant value for our target audience:
- **Quantifiable risk over time:** moving beyond static assessments, the model allows for projecting the probability distribution of being in different risk states at future points in time for state vector st+k. This provides a more dynamic, quantifiable view of risk crucial for risk and insurance professionals.
- **Scenario analysis and mitigation prioritisation:** by adjusting parameter values within the model, we can simulate the impact of different mitigation strategies. For instance, how does investing in faster internal patching (improving our effective PV parameter) change the probability of reaching a 'Compromised' state within the next quarter? How does replacing a component with a high VCS and low CAM score with a better-maintained alternative alter the risk trajectory? This helps executives and architects prioritise investments. The nth-order aspect allows us to see how a sequence of events (e.g., repeated failure to patch, combined with a vendor incident) impacts future risk, which a simple first-order model might miss.
- **Let's illustrate the conceptual value with a simplified nth order idea:** Assume our system's state regarding a critical third-party library depends on its current vulnerability status (V_t: Vulnerable/Not Vulnerable) and whether it was patched in the previous period (P_{t-1}: Patched/Not Patched). This is a second-order dependency on the patch history.

Our simplified 'system state' could be (V_t, P_{t-1}). For instance:
- ***State A:*** (Not Vulnerable, Patched) ideal state
- ***State B:*** (Vulnerable, Patched) new vulnerability found, previous one was patched
- ***State C:*** (Vulnerable, Not Patched) new vulnerability found, and previous one wasn't patched (potentially higher risk)
- ***State D:*** (Not Vulnerable, Not Patched) currently no known vulnerability, but historical patching failure (might indicate systemic issue).

The transition probability to the next state (V_{t+1}, P_t) depends on the *current combined state* (V_t, P_{t-1}). For example, the probability of transitioning to a 'Compromised' state might be significantly higher from State C (Vulnerable, Not Patched historically) than from State B (Vulnerable, Patched historically), even if the current vulnerability is the same. This captures the cumulative risk of poor security hygiene. The transition probabilities would be influenced by our selected parameters:
- A low PV parameter (slow patch velocity) increases the probability of transitioning *to* states where P_t is 'Not Patched' or remaining in such states.
- A high VCS parameter (more vulnerabilities) increases the probability of transitioning *to* states where V_{t+1} is 'Vulnerable'.
- Poor SAR (analysis results) might increase the probability of transitioning from 'Not Vulnerable' to 'Vulnerable' unexpectedly.

- **Improved communication:** The Markov framework provides a clear, visual (state diagrams) and quantitative (transition matrices, state probability vectors) way to communicate complex supply chain risk to senior executives and boards. Instead of vague hand-waving about 'third-party risk', you can discuss the probability of transitioning to undesirable states and the impact of mitigation efforts on these probabilities. Risk and insurance professionals can use this probabilistic output to better understand potential exposures and model financial impact.
- **Focus on improvement tracking:** The reliance on measurable parameters directly supports tracking improvements over time. Are the average patch velocities of our key open-source components improving? Is the aggregate vulnerability score of our third-party libraries decreasing? Are our vendors' security audit scores improving? These metrics, linked to the Markov model, provide tangible evidence of progress in managing supply chain risk.

Illustrative example: risk in cyber security platform libraries

Let's apply this concept with a simplified example focused on third-party libraries and open-source modules used in developing a cyber security platform (e.g., an endpoint detection and response agent or a security information and event management (SIEM) system). These platforms are particularly sensitive as they handle critical data and often require deep system access. Assume we focus on a set of core libraries for encryption, network communication and data parsing.

Simplified states:

- **S_0:** All core libraries are at the latest version with no known critical or high vulnerabilities.
- **S_1:** A new *high-severity* vulnerability (e.g., CVSS > 7.0) is publicly disclosed in one of the core libraries.
- **S_2:** The vulnerability from S_1 is actively being exploited in the wild, *or* a successful proof-of-concept exploit is available, *and* our platform version uses the vulnerable library.
- **S_3:** The exploitation attempt targeting the vulnerability in S_2 is successful *within our deployed platform*, leading to initial compromise (e.g., unauthorised access, data exfiltration from the agent, disruption of SIEM data processing).
- **S_4:** The compromise has propagated or resulted in a significant business impact (e.g., widespread agent compromise, major SIEM data integrity loss, regulatory notification required).
- **S_5:** The issue has been detected, contained, and mitigated (e.g., patched version deployed, incident response complete). (This would likely transition back towards S_0 over time).

Relatable parameters influencing transitions

Let's pick a few parameters and see how they influence transitions, considering a simple second-order dependency ($n = 2$), meaning the probability of the next state depends on the current state and the state in the previous time step.

- **Parameter P_1 (Technical, PV):** Average time for library maintainers (OS or Commercial) to provide a patch for high-severity vulnerabilities (e.g., measured in days). *Lower P_1 is desirable.*
- **Parameter P_2 (Technical, CAM):** Cumulative number of critical/high vulnerabilities found in this library over the past 12 months. *Lower P_2 is desirable.*
- **Parameter P_3 (Operational, SAR):** Frequency of internal security scanning (SAST/SCA) of the integrated libraries (e.g., scans per week). *Higher P_3 is desirable.*
- **Parameter P_4 (Business – CSRE):** Vendor support level for commercial libraries (e.g., premium support with guaranteed security patch SLAs versus best-effort). For OS, consider the health of the community and existence of dedicated security contributors. *Higher P_4 is desirable.*

Illustrating second-order transitions (conceptual)

Consider the transition from S_1 (vulnerability disclosed) to S_3 (initial compromise): $P(S_3 \mid S_1, S_2)$. The probability isn't just about being in S_1 now; it's about the *history*.

- If the system was in S_0 at *t-1* (fully patched previously), transitioning to S_1 at *t* might have a lower probability of quickly hitting S_3 if internal processes triggered by $S_0 \rightarrow S_1$ transition are swift (e.g., automated

alerting and patching). This swiftness relates to internal operational parameters not explicitly listed but influenced by P_3 (scanning helps detection) and P_4 (vendor support helps getting patches).

- If the system was in S_1 at *t-1* (vulnerable last period) and is *still* in S_1 at *t* (vulnerability remains unpatched), the probability of transitioning to S_3 is likely *much higher*. This persistent vulnerability is a cumulative risk captured by the memory. A low P_1 (slow patch velocity) from the library maintainer makes this persistent S_1 state more likely. A high P_2 (history of many vulnerabilities) might also increase the likelihood of *this specific* vulnerability being exploited quickly, based on attacker focus.
- The transition matrix for a second-order chain becomes complex, operating on pairs of states; however, the *insight* is that the probability of a bad outcome (like S_3) is higher not just when a vulnerability exists (S_1), but when that vulnerability is combined with a history of slow patching (low P_1 from vendor/OS project), a history of many vulnerabilities in that component (high P_2), or infrequent internal scanning (low P_3) leading to delayed detection and remediation.

The value of the Markov model here is:

- **Predicting risk trajectories:** Based on observed parameters (P_1, P_2, P_3, P_4), we can estimate the transition probabilities and project the likelihood of being in states S_2, S_3, S_4 over the next week, month, or quarter.
- **Evaluating parameter impact:** We can quantify how much a hypothetical improvement in P_1 (e.g., vendors/OS projects reducing patch time by 50 per cent) or P_3 (increasing internal scanning frequency) would reduce the probability of reaching S_3 or S_4. This provides data for business cases for investing in better vendor contracts, automated security tooling, or contributing to open-source security.
- **Continuous monitoring:** By continuously measuring these parameters, the model can be updated, providing a near real-time assessment of how the supply chain risk profile is evolving, which is far more valuable than annual audits.
- The equations, while complex in full form, conceptually show the state vector s_{t+1} depending on values of vectors st and s_{t-1}, mediated by transition probabilities influenced by parameters P_1 – P_4.

For illustrative purposes, we could show a simplified transition probability calculation: $P(S_3, t+1 \mid S_1, t, S_1, t-1) = f(P_{1t}, P_{2t}, P_{3t}, P_{4t}, \textit{External Threat Level}_t)$, where *f* is some function that increases with lower P_1, higher P_2, lower P_3, lower P_4, and higher external threat levels. This clearly links the business/technical parameters to the likelihood of a critical risk transition, resonating with all parts of the target audience.

Challenges and limitations revisited

Despite the powerful abstraction, it's crucial to be realistic about the challenges:

- **Data availability and quality:** Obtaining reliable, timely data for all parameters, especially those dependent on opaque third and fourth parties (like their true patch velocity or internal incident history), is extremely difficult. SLAs often don't mandate sharing this level of detail, and verifying provided data is hard.
- **Parameter selection and weighting:** Choosing the right parameters and understanding their relative influence on transitions is complex and may require significant domain expertise and potentially historical incident data (which is often scarce for supply chain issues).
- **Estimating transition probabilities:** Calculating accurate transition probabilities requires historical data on state changes and parameter values. For rare, high-impact events (like a fourth-party compromise propagating), this data is scarce. Initial probabilities may rely on expert judgment, industry benchmarks and assumptions, which introduce uncertainty.
- **Model complexity versus granularity:** Balancing the desire for a detailed, high-order model that captures complex dependencies with the need for a manageable number of states and parameters is a constant trade-off. Modelling too much leads to intractability; modelling too little oversimplifies the risk.
- **Unknown unknowns:** Markov models inherently deal with known states and probabilistic transitions between them. They struggle with completely unforeseen

events, such as zero-day exploits in critical, widely used software components where no prior 'Vulnerable' state was known, or malicious code injected into an open-source project by a new, previously unknown contributor.

The never-ending aspect of third- and fourth-party risk means we can never achieve perfect visibility or a perfectly predictive model; however, the goal is not perfection, but significant improvement over current methods.

Conclusion: towards a more intelligent approach

Cyber security supply chain risk, particularly the intricate dependencies introduced by third-party software libraries and open-source modules, presents a formidable and seemingly endless challenge. Relying solely on static assurances like SLAs or point-in-time audits is insufficient in a dynamic threat landscape.

Abstracting this risk as an nth-order Markov problem offers a structured and potentially powerful alternative. By defining relevant risk states and focusing on a select range of measurable, relatable business and technical parameters – such as vulnerability velocity, patch cycles, code analysis results, vendor security posture and incident history – we can begin to estimate the probabilities of transitioning between these states. While the inherent opacity of organisational boundaries and the depth of software dependencies make perfect modelling impossible, this approach provides significant value:

- It enables a more quantitative and dynamic understanding of supply chain risk over time, moving beyond static snapshots.
- It supports scenario analysis to evaluate the potential impact of different threats and the effectiveness of proposed mitigation strategies.
- It helps prioritise investments in risk reduction by identifying which parameters have the greatest influence on reducing the likelihood of undesirable outcomes.
- It provides a framework for continuous monitoring and tracking of supply chain security posture based on measurable indicators.
- It facilitates clearer and more impactful communication about complex risks to senior executives and stakeholders.

For senior business leaders, risk professionals, and technical architects, adopting such a probabilistic, parameter-driven approach, even in a simplified form, transforms supply chain risk from an overwhelming, nebulous threat into a problem that can be analysed, managed, and strategically addressed. It acknowledges the reality of shared risk and imperfect information, while providing a robust framework for making informed decisions in an interconnected world. By focusing on what can be measured and tracked, organisations can move beyond the illusion of control offered by static agreements and build more resilient digital supply chains. The journey towards perfect visibility may be never-ending, but informed abstraction provides a vital road map. •

References

1. C. J. Wooff and J M. Lambert, 'Modeling the Reliability of Complex Systems Using Markov Chains,' *IEEE Transactions on Reliability*, Vol. 38, No. 2, pp. 226-231, Jun, 1989. doi: 10.1109/24.25593
2. E. Jonsson, 'Development of a Vulnerability/Intrusion Taxonomy for Quantifiable Security,' *Computers & Security*, Vol. 16, No. 4, pp. 329-339, 1997. doi: 10.1016/S0167-4048(97)80540-7
3. F. Wu, J. Bi, and B. Fu, 'Cyber Supply Chain Risk Management: A Survey,' in Proc. 2017 IEEE Conference on Energy Internet and Energy System Integration (EI2), 2017, pp. 1-6. doi: 10.1109/EI2.2017.8246976
4. R. S. Chen, J. M. Outkin, M. D. Porter, and C. L. Hoover, 'A Framework for Evaluating Supply Chain Cyber Risks,' *Journal of Cyber Security*, Vol. 3, No. 2, pp. 95–107, Jul, 2017. doi: 10.1093/cybsec/tyw012
5. V. Bollegala and S. Y. Hwang, 'Modeling Cyber security Risk Propagation in Supply Chains,' in Proc. 2018 IEEE International Conference on Big Data (Big Data), 2018, pp. 3146-3155. doi: 10.1109/BigData.2018.8622364
6. T. C. Walljasper, 'Quantitative Risk Management: A Practical Guide for Cyber Security Leaders,' *IT Professional*, Vol. 21, No. 4, pp. 24-31, Jul, 2019. doi: 10.1109/MITP.2019.2918053
7. NIST, 'Cyber security Supply Chain Risk Management Practices for Systems and Organizations,' NIST Special Publication 800-161r1, May, 2022. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800- 161r1.pdf
8. M. A. Tanner, 'Using Markov Chain Monte Carlo,' *Statistical Science*, Vol. 11, No. 3, pp. 205-217, Aug, 1996.
9. F. Hakami and A. R. Hurson, 'A Review of Cyber security Risk Analysis Methods,' *Journal of Network and Computer Applications*, Vol. 161, 102641, Jul, 2020. doi: 10.1016/j.jnca.2020.102641
10. S. Zhao, Y. Zhou, and M. Xie, 'Reliability Modeling and Analysis of Software Systems Considering Dependency,' *Journal of Systems and Software*, Vol. 83, No. 12, pp. 2441-2453, Dec, 2010. doi: 10.1016/j.jss.2010.07.047
11. T. W. Archibold, 'The Role of Cyber Risk Quantification in Third-Party Risk Management,' *ISACA Journal*, Vol. 6, 2021.

Help us, tech bro!

BY AMBERLEY BRADY, FOUNDER, REAL FOOD PRICE

Australia's agricultural sector is ripe for a technological revolution. This isn't just another industry waiting for disruption – this is our chance to transform one of the nation's most essential foundations using cutting-edge innovation.

The timing couldn't be more perfect. Climate challenges are intensifying, supply chains are becoming complex, and farmers are demanding smarter solutions. This creates an incredible opportunity for tech professionals and cyber security experts to make a real, tangible impact.

We're not just building apps – we're creating the future of food production! Imagine deploying Internet of Things sensors across Australian farms, delivering real-time soil health data directly to farmers' fingertips. But here's the kicker – unlike those amateur startups storing passwords in plain text, we're talking bulletproof encryption and security protocols that would make government agencies jealous.

We're on the brink of unleashing artificial intelligence (AI) systems so sophisticated that they can predict pest invasions and weather patterns with mind-blowing accuracy. This isn't just technology for technology's sake – this is about merging Silicon Valley innovation with agricultural wisdom to create something extraordinary.

But it's not just about tools – it's about interconnected ecosystems that work seamlessly in unison. Autonomous tractors outfitted with precision GPS could revolutionise the way that fields are ploughed and seeds are sown. Vertical farming methods could bring fertile harvests to urban centres, shrinking the gap between producers and consumers. Alongside this, blockchain technology could offer transparent supply chains, ensuring farmers are compensated fairly while consumers know that their food isn't compromised.

We are at the point where we need everyone in cyber on board. Agriculture has long been characterised as a traditional, slow-to-change industry that lags significantly behind other sectors in technology adoption – kind of like Internet Explorer trying to keep up with Google Chrome, but with tractors.

When we think of how we can fix this problem, it's apparent that we need to gain the interests of the big end of tech and, importantly, all tech bros. But hold on – before you roll your eyes at needing a tech bro, hear me out. Agriculture today faces challenges that are as multifaceted as they are urgent. Climate change, soil depletion and labour shortages aren't going anywhere, and the solutions must be as bold as the problems are daunting.

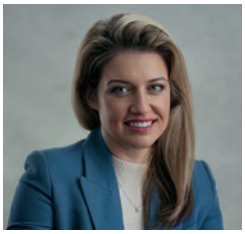
Maybe the tech bro isn't all puffer vest and ego. Perhaps they are the unorthodox ally who could tackle agriculture's most stubborn puzzles with the same vigour they apply to coding groundbreaking apps or engineering self-driving cars. By applying their knack for innovation and disruptive thinking, this archetype could help propel farming into a new era, where ancient practices meet modern tech.

On the ground, the agriculture sector faces unique barriers to technological advancement. Farmers often operate on paper-thin profit margins, making large capital investments financially risky, kind of like betting your entire budget on non-fungible tokens in 2022. Unlike tech companies that can pivot quickly, agricultural decisions have long-term consequences tied to seasonal cycles spanning years rather than months.

Rural infrastructure presents another major obstacle. Many farming regions have internet connectivity so spotty it makes dial-up look lightning fast. Without robust connectivity, farmers cannot fully utilise GPS-guided tractors, drone monitoring systems, or real-time weather and soil data that could optimise their operations.

Meanwhile, governments are being overwhelmed – not through any fault of their own – and are left holding a chocolate teapot trying to address the cascading environmental disasters that modern agriculture both contributes to and suffers from. Political cycles are too short for long-term ecosystem restoration, regulatory agencies are underfunded and often captured by industry interests, and international cooperation moves at a glacial pace while forests burn and species disappear.

This is where an unlikely saviour emerges: the tech industry's obsession with longevity and personal optimisation. Tech billionaires worried about consuming pesticide residues in their organic kale smoothies are funding research into precision fermentation and cellular agriculture. Their desire for the purest, most nutrient-dense foods is driving investment in soil microbiome restoration and advanced hydroponics. The same individuals obsessively tracking their biomarkers are naturally drawn to



Amberley Brady

technologies that can produce food with precise nutritional profiles and provable zero contamination.

The farming community has looked after us through floods, fires and COVID-19 – they've been more reliable than cloud services during peak usage. We need our tech moguls with their deep pockets and impatience with slow progress to have their moonshot moment. Precision agriculture systems can satisfy their love of data and quantified optimisation. Personally, who doesn't love tracking something grow?

The consequences of this tech gap extend beyond individual farms. As global food demand increases and climate change creates new agricultural challenges, the need for more efficient, sustainable farming practices becomes critical and, for Australia, a national security issue. Countries that successfully modernise their agricultural sectors gain competitive advantages, while those that lag risk food security issues. Drought cycles are intensifying, extreme weather events are wiping out entire seasons, and who can forget the $12 cabbages? Traditional farming methods are hitting their limits just when we need to feed more people with fewer resources – it's like trying to mine bitcoin on a Game Boy.

This is exactly the kind of 'impossible' problem that can generate industry excitement. The kind that requires moonshot thinking, massive scale, and the audacity to reimagine entire systems from scratch.

The industry has proven you can scale global platforms to billions of users. Now, we need you to scale food production to feed billions of people sustainably. You've disrupted commerce, communication and transportation. Agriculture is waiting for its Uber moment.

The Australian Strategic Policy Institute has called out that Australia's agricultural powerhouse feeds more than 70 million people globally through one of the world's least-subsidised food systems. Right now, it feels like the perfect storm where we are waiting for something to strike – except this time, it's not just our software supply chain at risk, it's our actual food supply chain.

Digital infrastructure has now started to form the network of our food system – precision agriculture, automated supply chains, satellite monitoring, and blockchain traceability. This technological dependence creates new attack vectors that hostile actors could exploit, including cyber warfare targeting food system networks, critical infrastructure attacks, and technology supply chain weaponisation.

For Australia, this isn't just about creating a more efficient agricultural system; it's about fortifying a backbone of national resilience. Every step towards innovation in agriculture is a step towards mitigating risks that threaten the very fabric of our society.

This generation of Australian farmers might be the last if we don't act now. But I have hope that with your innovation, your capital, and your relentless drive to solve impossible problems, our farmers could also be the first generation of truly sustainable, tech-enabled agricultural pioneers. Don't let them fail harder than Google+.

The gloves are off. The future of Australian farming hangs in the balance. Will you answer the call? •

About the author

***Amberley Brady**, an astute industry professional with extensive experience in public policy, founded Real Food Price in 2024 in response to identified structural inefficiencies within Australia's food supply chain. Recognising the critical need for market transparency, she established this data-driven platform to address the competitive imbalance affecting both producers and consumers.*

Ghosts in the machine: why we should study folklore to understand modern threat actors

BY MARYAM SHORAKA

How hacker groups use myth-making, symbols, and narrative to influence and intimidate.

In the pantheon of cyberthreats facing Australia today, something peculiar emerges when we examine the adversaries themselves. Beyond the sophisticated technical capabilities and evolving attack vectors lies a fascinating truth: today's threat actors are master storytellers, weaving mythologies as old as human civilisation itself. From the Guy Fawkes masks of Anonymous, to the hydra-headed persistence of ransomware groups, modern cybercriminals are drawing from humanity's oldest playbook: folklore.

The Australian Signals Directorate's (ASD's) latest Annual Cyber Threat Report reveals that malicious cyber actors continue to target Australian governments, critical infrastructure, businesses and households, with the ASD responding to more than 1100 cyber security incidents in the past year. Yet, while we dutifully catalogue their technical methodologies and defensive countermeasures, we're missing a critical dimension of threat intelligence: the anthropological.

The ancient art of fear

Mythology comes from the Greek words 'mythos' ('story of the people') and 'logos' ('word'), and is defined as the spoken (later written) story of a culture. Central to these stories are supernatural characters whose purpose is to convey a message, and these figures were expressions of the fears and hopes of the people.

This definition could easily describe modern ransomware groups. Consider how these criminal enterprises name themselves: Medusa,

capable of turning victims to stone with a glance; Hydra, growing two heads for every one severed; and Cerber, the three-headed guardian of the underworld. These aren't coincidental choices – they're deliberate psychological weapons.

The Clop ransomware group employs double extortion tactics, while the Black Basta ransomware group, emerging in early 2022, quickly rose to prominencewith more than 100 victims in just its first few months. But beyond their technical capabilities, these groups understand something cyber security professionals often overlook: names have power.

In the Philippines, parents once invoked the Manananggal – a vampire that detaches its torso to hunt – to keep children obedient. Today's ransomware groups similarly weaponise ancient fears, but for modern ends. When a CISO receives notification that 'Medusa' has encrypted their network, they're not just dealing with malware – they're confronting a mythological force designed to paralyse decision-making.

The symbolism of intimidation

Anonymous is recognisable by their symbols – Guy Fawkes masks and the slogan 'We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.' They claim their work is about advocating for freedom of speech, government transparency, internet freedom and social justice.

The Guy Fawkes mask isn't merely theatrical – it's a carefully chosen symbol connecting modern hacktivism to historical rebellion. Fawkes attempted to blow up parliament in 1605, and his mask now represents the faceless many challenging authority. This isn't happenstance; it's sophisticated narrative construction.

Consider how corporations unconsciously understand mythological branding. Nike's swoosh is derived from the wing of the Greek goddess of victory, Versace uses the Medusa head, and Maserati employs Neptune's trident as symbols of vigour and strength. If legitimate businesses recognise mythology's persuasive power, we must acknowledge that threat actors – equally concerned with psychological impact – are employing the same principles.

The difference is intent. Where Nike inspires athletic achievement, groups like LockBit (suggesting impenetrable security turned against victims) or REvil (phonetically 'Reveal' and 'Evil') deliberately evoke helplessness and malevolence.

The psychology of pack behaviour

Wolves are important figures in Native American cultures, with the wolf's dedication to its pack inspiring many beliefs. The Cheyenne, Lakota and other tribes tell stories of wolves as role models who taught people how to hunt, often involving mutual support between people and wolves.

Modern threat actors mirror this pack mythology. Cybercriminal groups that engage in cyber operations for financial gain operate similarly to wolf packs, with hacktivists motivated by political or ideological beliefs targeting organisations to disrupt operations as a form of protest.

This tribal structure isn't coincidental. Ransomware-as-a-Service operations function like mythological pantheons, with dominant groups licensing their capabilities to subordinate 'affiliates'. The psychological comfort of belonging to something larger than oneself – whether a wolf pack, mythological pantheon, or cybercriminal consortium – remains fundamentally human.

Advanced persistent threat (APT) groups exemplify this perfectly. Names like 'Cozy Bear' and 'Fancy Bear' aren't technical designations – they're tribal identifiers that simultaneously convey threat (bear) and approachability (cosy, fancy). These groups understand that effective psychological operations require both fear and familiarity.

The Australian context: learning from our own folklore

Australia faces unique challenges in this mythological battleground. With state-sponsored cyber actors persistently targeting Australian governments and critical infrastructure, and significant data breaches resulting in millions of Australians having their information stolen and leaked on the dark web, we need new approaches to threat intelligence.

Our own folklore also offers insights. Aboriginal Dreamtime stories, with their emphasis on consequence and interconnectedness, mirror modern cyber threats. Just as traditional stories warned

of disruption when cultural protocols were violated, modern threat actors exploit violations of digital protocol – unpatched systems, weak authentication, and inadequate backup procedures.

Identity fraud remains the leading concern for individuals, affecting 26 per cent of Australians, while business email compromise accounted for 20 per cent of reported cyber incidents. These aren't just statistics – they're modern manifestations of ancient fears about identity theft and deception that folklore has always addressed.

The narrative warfare dimension

Understanding threat actors through folkloric analysis reveals sophisticated narrative warfare. Nation-state actors intensified cyber espionage and added artificial intelligence to their arsenal in 2024, with China-nexus activity increasing by 150 per cent. These aren't merely technical developments – they're escalations in humanity's oldest competition: Whose story wins?

Chinese APT groups often adopt names referencing historical dynasties or cultural symbols, positioning their activities within centuries-old narratives of technological and cultural superiority. Russian groups frequently invoke folklore around bears and winter – symbols of endurance and inevitable victory. Understanding these cultural contexts provides crucial intelligence about adversary psychology and probable future behaviour.

When Lapsus$ recruited through Telegram and employed social engineering tactics that included 'MFA fatigue,' they weren't just exploiting technical vulnerabilities – they were weaponising human psychology through familiar patterns of exhaustion and surrender that appear throughout folklore.

Practical implications for CISOs

This folkloric lens offers practical defensive value. Traditional threat intelligence focuses on indicators of compromise and tactics, techniques, and procedures. But understanding mythological motivations provides strategic insight into adversary persistence, likely escalation paths, and psychological pressure points.

For instance, groups invoking regenerative mythology (like Hydra-themed ransomware) signal likely persistence through law enforcement action. Understanding this can help organisations prepare for prolonged engagement rather than expecting single-point solutions.

Naming conventions also reveal targeting priorities. Groups adopting predatory folklore (like spiders, wolves and ravens) typically focus on opportunistic attacks, while those invoking protective or justice-themed mythology (like shields, scales and swords) often engage in targeted operations against specific sectors or ideologies.

Building folkloric threat intelligence

CISOs should integrate anthropological analysis into threat intelligence programs. This means:

- **Understanding adversary cultural contexts:** Chinese APT groups operating during Chinese New Year often reduce activity, not for technical reasons, but for cultural ones. Russian groups may intensify operations around historical remembrance dates.
- **Analysing symbolic communication:** When groups change names or adopt new symbols, they're often signalling operational shifts. The transformation of DarkSide into BlackMatter wasn't just rebranding – it was mythological evolution, moving from shadow-based to substance-based symbolism.
- **Recognising psychological campaigns:** Groups that heavily invest in mythological branding typically prioritise psychological impact over pure technical sophistication. This suggests different defensive priorities and incident response approaches.

The counter-narrative challenge

The steady increase in incident numbers has prompted increased regulatory focus, with greater recruitment of people with cyber knowledge to boards, and increased regulatory scrutiny on compliance and investigations.

But regulatory compliance alone won't counter mythological warfare. Australia needs its own positive cyber mythology – stories that inspire resilience rather than fear, collaboration rather than isolation.

Consider how effective cyber security awareness campaigns could draw from

Australian folklore. The concept of 'mateship' during bushfire season – neighbours checking on each other, sharing resources, maintaining communications – directly translates to cyber security hygiene. The traditional Aboriginal practice of controlled burns to prevent larger fires mirrors proactive threat hunting and vulnerability management.

The eternal human element

The Albanese Government has committed $15–20 billion to 2033–34 to enhance our cyber domain capabilities, with significant investment providing greater visibility into threats to critical infrastructure. Technology and investment are crucial, but they're insufficient without understanding the human dimension of cyber conflict.

Threat actors succeed not just through technical sophistication, but through psychological manipulation rooted in humanity's oldest fears and aspirations. They understand that cyberspace isn't separate from human culture – it's an extension of it, complete with the same mythological patterns that have shaped human behaviour for millennia.

By studying folklore, we gain insight into adversary psychology, operational motivations and strategic objectives that purely technical analysis misses. More importantly, we remember that cyber security is fundamentally about protecting human institutions, relationships and values – the same things that folklore has always sought to preserve.

The ghosts in our machines aren't malfunctions – they're ancient patterns of human behaviour, digitally manifest. Understanding them isn't just academic curiosity; it's an operational necessity. In the mythology of cyber conflict, the side with the better story often wins.

It's time we started paying attention to the stories our adversaries are telling – and crafting better ones ourselves. •

The author acknowledges that understanding adversary mythology doesn't diminish the serious technical challenges of cyber security, but rather adds a crucial human dimension to our defensive strategies. This analysis is intended to complement, not replace, traditional threat intelligence methodologies.

About the author

***Maryam Shoraka** is Head of OT Cybersecurity Operations and a seasoned security executive with extensive experience building world-class 24/7 security operations centres and developing cyber resilience strategies. Having previously served as Acting CISO and Head of Cybersecurity Operations, Shoraka now specialises in helping organisations to rapidly recover from high-impact cyber incidents.*

Resources and references

Australian Government sources:

- Australian Signals Directorate, Annual Cyber Threat Report 2023–2024, www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024
- ASD Cyber Threat Report 2022–2023, www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023.

Threat intelligence sources:

- CrowdStrike, 2025 Global Threat Report, www.crowdstrike.com/en-us/global-threat-report/
- Recorded Future, 'Most Popular Ransomware Groups to Watch (Updated 2025)', www.recordedfuture.com/threat-intelligence-101/cyber-threats/ransomware-groups
- BlackFog, 'The Top 10 Ransomware Groups of 2023', www.blackfog.com/the-top-10-ransomware-groups-of-2023.

Academic and cultural sources:

- World History Encyclopedia, 'Twelve Menacing & Protective Mythological Figures', www.worldhistory.org/article/1457/twelve-menacing--protective-mythological-figures/
- Designhill, 'Popular Logo Symbols And Their Shocking Mythological Stories', www.designhill.com/design-blog/popular-logo-symbols-and-their-shocking-mythological-stories.

Industry analysis:

- Governance Institute of Australia, 'Cyber in 2023 and 2024: What we've seen and what's to come', www.governanceinstitute.com.au/news_media/cyber-in-2023-and-2024-what-weve-seen-and-whats-to-come/
- BDO Australia, 'Top cyber security threats and predictions for 2025', www.bdo.com.au/en-au/insights/cyber-security/top-cyber-security-threats-and-predictions-for-2025.

Cyber security on a shoestring

BY DINESH VELUSAMY

How Australian organisations can build resilient defences without breaking the bank.

Dinesh Velusamy

Australia's digital backbone is under siege. With cyberthreats rising in frequency and sophistication, and legislation like the *Security Legislation Amendment (Critical Infrastructure) Act 2021*, and the expanded *Security of Critical Infrastructure Act 2018* (SOCI) reforms now in force, the pressure on Australian organisations has never been more significant.

However, many businesses – especially those in critical sectors – face a sobering reality: their cyber security ambitions are often more significant than their budgets. So, how can you design a business-ready cyber security framework that is compliant, scalable, and resilient without spending like a Big Four bank? The answer lies in smart design, open-source tools, automation and a relentless focus on risk.

Start with the rules: understand what you must defend

Before considering firewalls or detection tools, it is essential to comprehend what needs protection and your legal obligations. The SOCI reforms impose stringent requirements on businesses in energy, health care, communications, transport, and financial services industries. These obligations involve identifying critical assets, managing risks effectively, and promptly reporting cyber incidents.

The first step? Map your assets

Know what is critical, what systems connect to it, and where your blind spots are. You do not need a six-figure tool to do this basic network scanning, and asset discovery tools like OpenVAS or Nmap can help you get started.

Once you know what's at risk, align your controls with frameworks like the Australian Cyber Security Centre's (ACSC's) Essential Eight. Think of this as your minimum viable security strategy. It's free, widely accepted, and backed by the government.

Secure the network: shrink the attack surface

If attackers can't move freely through your systems, they can't cause much damage. This is the thinking behind micro-segmentation, which divides your network into smaller zones so that even if someone breaks in, they cannot go far.

Pair that with least-privilege access controls, strong identity management, and always-on encryption (Transport Layer Security 1.3 is your friend), and you've got the skeleton of a Zero Trust architecture – even if you don't have a Gartner-sized budget.

Free and open-source tools like pfSense can act as powerful firewalls. To protect remote access, combine them with secure VPN tunnels like strongSwan.

Think like an attacker: model the threats

Threat actors, whether cybercriminals or state-backed groups, do not play fair. They exploit gaps, misconfigurations and human errors. That's why threat modelling should be an integral part of your design process, not an afterthought.

Use models like STRIDE or MITRE ATT&CK to understand potential adversary paths. Then, layer your defences accordingly – from endpoint protection, to network monitoring and cloud hardening.

Want threat intelligence without the price tag? Tap into free feeds from AUSCERT, ACSC, and AlienVault OTX. Combine them with

Wazuh (an open-source security information and event management/endpoint detection and response platform) to create a functional detection and response engine at a fraction of the commercial cost.

Resilience is the real return on investment

Even the best defences can be breached. That is why resilience – your ability to respond, recover and keep operating – is where the real value lies. You do not need a $1 million disaster recovery solution. You need a tested business continuity plan, a clear incident response playbook, and automated backups that you can restore.

Follow the 3-2-1 rule: three copies of your data, two formats, one offsite. Store backups in cost-effective cloud cold storage like AWS Glacier, and script your recovery drills using open tools or even basic shell automation.

Let automation do the heavy lifting

Cyber teams are stretched thin. Automation isn't a luxury – it is survival.

Start small. Use scripts to block suspicious IPs, alert on failed login attempts, or pull system logs into a central location. Explore tools like Cortex XSOAR Community Edition to build workflows and response playbooks.

Want to go a step further? Machine learning libraries like scikit-learn or TensorFlow can be used to detect anomalies in network traffic or user behaviour. You don't need a data science team to get started, just curiosity and a few hours of Python.

Cyber security does not have to be expensive ... just smart

Too often, cyber security is viewed through the lens of expensive platforms and enterprise licenses. But the fundamentals – knowing your assets, defending in layers, building resilience and responding fast – are achievable even on modest budgets.

In a world where compliance is mandatory and threats are inevitable, intelligent design, open-source tools, and automation can level the playing field.

Whether you're securing a hospital, a logistics firm, or a regional power grid, remember this: the most resilient organisations aren't always the biggest spenders. They are the ones who prepare with intent – and execute with discipline. •

About the author

Dinesh Velusamy *is a seasoned technologist and business leader with more than 20 years of global experience in cyber security, artificial intelligence and IT service management. He is currently pursuing a PhD, and holds master's degrees in IT and cyber security, seamlessly integrating academic insight with practical application. As a GRC Specialist at Wurth Australia, Velusamy leads cyber security initiatives, drives IT compliance, promotes user education and cultivates strategic external partnerships. His work is grounded in aligning governance frameworks with innovation and resilience.*

A day in the life of an SOC manager: people, pressure and priorities

BY KUNAL MAKWANA

The day always starts with optimism, good intentions, and a sweet Indian masala tea that – spoiler alert – will never be finished while it's still hot.

It's 7:45 am. I am coming back from dropping my son at the bus stop, and sit in my chair, half expecting a quiet morning of patch validation and metric reviews. Instead, my phone looks like it's been hit by a denial-of-service attack; messages are pinging like a slot machine, and one of the team members says our ticket management system dashboard is lit up like a Christmas tree in July. Welcome to the security operations centre (SOC) – where the only constant is chaos, and our motto might as well be, 'If it's quiet, you've probably missed something.'

For me, being a SOC manager isn't just about managing security; it's about leading with empathy, staying proactive, and being approachable and responsive in the face of pressure.

The morning rush: tea/coffee, context, and chaos

Early in the morning, usually around 8 am, the team is live. The shift handover follows, often with a mix of bleary-eyed humour and grim updates. Someone casually mentions, 'It wasn't that bad ... until 3:12 am.'

Our first few minutes are for debriefing overnight alerts and aligning priorities. The SIEM has flagged a handful of suspicious logins, one of which turns out to be our own executive logging in from Bali ... again.

The team skims dashboards like a stockbroker watching the market. CPU spikes? Suspicious lateral movement? Network egress anomalies? Check, check, check. This is where the triage begins.

As I often say: 'Charity starts at home, intelligence starts with logs.' No decision is made without context, and context lives in our telemetry.

From logs to leadership: translating action into assurance

Technical depth is important, but if you're not turning logs into language stakeholders to understand, you're missing half the job. Let's say that detection rules recently flagged multiple failed logins to a legacy HR system – low fidelity in a busy environment, but got traced to a misconfigured VPN client.

Rather than just closing the case, we documented the context, shared the remediation plan and explained the potential risk it posed. This communication builds trust. In security, transparency isn't weakness – it's currency.

Maintaining stakeholder confidence means two things: sharing what matters and never blindsiding them. I aim to anticipate their questions before they ask. It's not just about being proactive with threats, it's about being proactive with people.

Team dynamics: leadership with empathy (and a bit of sarcasm)

One of my core strengths as a leader is empathy. Yes, I've been told I'm too nice, but here's the thing: for me, empathy gets results. People work harder when they feel heard. My job is to make them feel safe to fail, confident to try and empowered to lead.

Reading *The Self-Aware Leader* by John C. Maxwell only reinforced this mindset. It's a brilliant book that encourages leaders to understand their strengths and weaknesses,

and the impact they have on others. I'm grateful for the perspective it offers – especially in a field where stress is high and human connection is often overlooked.

Every SOC has its personalities: the log magician, the packet whisperer, the fresh grad with 600 tabs open. And that's great. My role is to orchestrate all of it in a coherent rhythm. Accountability starts with me. If something slips, I will own it. That's non-negotiable.

Beyond the alerts: the SOC's hidden inbox

You thought SOC work was just an alert? That's adorable. Here's a sampling of the unexpected:

- **Random asks from stakeholders:** 'Can you check if someone opened this email … six months ago?'
- **Audit requests**: Usually due yesterday, complete with acronyms that would make an alphabet soup blush.
- **Internal investigations:** Sensitive, messy and always under the radar.
- **Calendar roulette:** People send meeting invites without checking if we're already fighting cyber fires. Classic.

These aren't distractions – they're part of the job. But they do stretch the boundaries of what it means to be a SOC leader.

My 5W strategy helps here. Every request gets this filter before we jump in. Context is king.

Incident response: firefighting in real time

Every alert is a potential headline waiting to happen. So, we treat them with the right balance of urgency and scepticism.

We run scenarios, red team exercises, and tabletop drills, but nothing beats the adrenaline of the real thing: indicators lighting up, analysts shouting over Zoom, the ticking clock of containment windows.

And through it all, my job is to keep calm, delegate clearly and escalate wisely. Panic is infectious. So is clarity.

Bridging the technical–business divide

Part of my job is explaining to executives why 'nothing happened today' is actually the result of hundreds of actions and decisions. When it comes to cyber risk, silence is a success.

But storytelling matters. Dashboards don't impress boards. Outcomes do. I translate our SOC metrics into business-relevant impact – and make sure the right people understand what's at stake.

That means owning the message, delivering it with relevance, and making it easier for others to take action on our insights.

Mental health and sustainable security

Burnout is real in this line of work. The pressure to always be 'on' takes its toll. So, I rotate shifts, enforce no-meeting zones, and check in on my team's emotional wellbeing. A SOC that can't breathe can't defend.

Being kind isn't soft, it's strategic. And it's how I get results.

Conclusion: a role that never sleeps (but occasionally smiles)

There are days when the work feels overwhelming, and nights when I dream in log queries. But this job matters, and leading with empathy, accountability and responsiveness has turned chaos into coordination.

I may never finish my tea, but I finish each day knowing our team made a difference. And, in the end, that's worth every ping, alert, and last-minute calendar invite. •

Special thanks to John C. Maxwell for The Self-Aware Leader *– an excellent reminder that strength starts with self-awareness.*

Note: The views expressed in this article are my own, based on personal experience, and do not necessarily reflect those of my current or past employer.

Apprenticeships in cyber security

BY TAVIENE CLARK-KENNEDY

I graduated last year, but I've had previous experience in IT, and was privileged and honoured to work for Apple, Microsoft, and Cisco. I've applied for hundreds of jobs this past year, because we all know that the so-called 'entry-level' roles in cyber security want you to have 3–5 years' experience and your CISSP.

Let's be realistic – it's called expectations. The big companies and recruiters need to stop holding unrealistic expectations for graduate roles. Meanwhile, at the top end of town, the experienced people are burning out (thanks to the cyber security skills shortage) because they are doing the job of five people, and they'll probably burn out and quit before they can train a willing graduate keen to absorb all their experience.

The tech companies, however, keep cutting off their noses to spite their faces and won't hire grads. Kate Kirwin, from She Codes Australia, pointed out several pertinent points in her keynote at BrisSEC recently: artificial intelligence (AI) is not taking everyone's jobs in cyber security; you need to hire grads; and you need to hire women! I've applied for many grad programs and internships. Sadly, you often have to apply for these two years ahead of time – so what do I do with my time when I graduate in early 2024, but have to wait two years before my internship in 2026? Should I volunteer for free to get experience on my résumé? Again, that's not realistic, as I still have to provide for my family and put food on the table.

Taviene Clark-Kennedy

When my older brother (who has ADHD like me) finished high school with poor marks, my parents encouraged him to apply for a trade. Trades, as we know, are recession-proof and you'll never be out of a job. He got an apprenticeship in the mines as a boilermaker–welder. He struggled all through high school – even though he is genius level in maths – because he has dysgraphia and dyspraxia. I have dyscalculia and should have gotten a trade and gone into hairdressing. So, we had a deal – he was two years older than me, and I used to do all his English assignments for him. When I was doing my final exams in Year 12 and going for a TE score after a week of exams, we got to English (my best subject) and I had an ADHD panic – blanked, froze, and wrote nothing for the entire exam! Luckily, I still managed to get a decent enough score and I was the first person in my family to go to university. So, off I went and studied psychology for six years.

Unfortunately, in my second year, my family shelled out an exorbitant amount of money for what was, unbeknownst to us, a second-hand computer housed in a brand-new shell. As a result, I started my learning journey with computers by constantly having to pull apart and fix my computer since we couldn't afford a call-out fee.

Here is what I believe to be the solution to the ongoing issue of cyber security shortages: apprenticeships! Yes – think of it this way – the journeyman trains the apprentice in everything and all things cyber security. They get hands-on knowledge as well as theoretical knowledge, get paid to do the training, and when finished their apprenticeship, they'll be at a level of knowledge and experience that companies will accept.

As everyone in cyber security seems to be neurodivergent, I'm going to go on an ADHD tangent and tell you a story. Whenever we go to a cyber security conference, my study buddy and I play a game called 'spot the neurotypical'. It's like Where's Wally – they

are very hard to find! What we need in our industry are certifications and qualifications that do not require exams, because ADHD people do not do well under exam stress. We'd be better off explaining concepts in person or demonstrating our understanding hands-on. Exams just show your ability to regurgitate information under stress – they don't show your understanding or your ability to apply that knowledge.

In their first year, hairdressers sweep floors and wash hair, but by the fourth year, they specialise and become a colourist or a cutter. Nurses do the same – they do placements in different areas and hospitals so they can decide what area to specialise in. My brother's boilermaker–welder apprenticeship was a combination of hands-on work at the mine, theoretical work at TAFE and industry placements. In his final year, his specialisation led him to become one of only six people in the world who could weld titanium. A week after finishing, he was green-carded by an American company to work on tour for two years as a professional bike mechanic.

We all know apprenticeship wages aren't fantastic, but at least you're earning while you're learning. It's better than volunteering just to show you have experience without getting paid.

We also need to look at talent identification – like in sports, where scouts go to schools to see who's excelling. Why not run CTFs at schools, or like ASIO used to do – hide code in crossword puzzles and see who cracks them? If we're going to solve the shortage, we need to be proactive and identify up-and-comers. We also need to do some PR – sell our industry! I agree with Kate Kirwin – we need a PR makeover. People think we wear hoodies and live in our mum's basement. We need to bring some ADHD sparkle to our image and make it more enticing – showcase the diversity of people and areas in our industry.

When Andrew Wallace MP spoke at one of our networking events last year at the Innovation Centre in Sippy Downs, I put it to him: the frustration of doing all this study with no job prospects. Why couldn't the government create an incentive program like they do for employing people with disability – where they pay employers to take on a graduate?

Cyber security apprenticeships would help address the skills shortage. Cyber is so broad – an apprenticeship could build vital foundational skills in areas like governance, risk and compliance; cryptography; ethical hacking; operational technology; digital forensics; programming; and more. Then, with some industry placement, people could specialise in their final year. The company could even pay for the certifications needed in that specialisation.

We know we have to go to all the conferences and networking events to get known in the industry. But it's hard – firstly, to afford all these events when you're not working, and secondly, because it's disheartening to keep seeing your grad mates when none of you have a job yet! As I've discussed with many people, once you're in, you're in – but the hardest part is getting your first break.

People who complete apprenticeships are usually hired by the company they trained with. So, having four years of paid learning, training under people with real experience, and gaining the skills and understanding the industry actually wants, would be motivating and reassuring for people trying to break in.

I've been fortunate to have been mentored twice a week in Brisbane since last year – I travel down from the Sunshine Coast because I'm that keen. When I met my mentor, Paul Rose, at an Australian Information Security Association meeting, I just asked if he would mentor me. He's mentored many people over the years and sees it as his duty to give back to the industry. Honestly, one of my fellow mentees did her cyber security training at TAFE, and I did mine at university – we both agreed we've learnt more in two hours with Rose than in two years of formal study. He goes deeper, gives real-life examples, and makes us do presentations to show our understanding.

Apprenticeships won't solve the cyber security shortage overnight, but at least they put people in the pipeline with the right training and experience. Instead of misleading new grads into thinking they'll walk straight into a high-paying job, we could build professionals with real, solid foundations.

Apprenticeships will give people a deep understanding of cyber security concepts and core skills to grow a successful career. Let's train them properly and build the cyber workforce we need. •

Winning the cyber budget – a hallmark of women in leadership

BY DENNY WAN AND MADHURI NANDI

Under the increasingly uncertain economic conditions in 2025, winning the cyber budget requires meticulous financial analysis of business impact from cyber incidents, supported by measurable reduction in attributable financial loss. Female leaders have a natural advantage in being good listeners, with attention to details in analysis[1]. In this article, we explain the paradigm shift in cyber risk management over the past decade, recognising cyber security as a business problem enabled by technology.

Budgeting decisions will be lost and won on the merit of business necessity, instead of macho threat language. We provide a high-level introduction to the Open FAIR cyber risk quantification (CRQ) standard, which is the only CRQ standard endorsed by the National Institute of Standards and Technology (NIST) under NISTIR 8286[2]. We explain the mission of the Australian Women in Security Network (AWSN) in nurturing the next generation of women leaders in security, and bolstering the resources available to members under the 2025 strategy, Voice of the Industry.

Cyber risk is a business problem

ISACA's paper, Reporting Cybersecurity Risk to the Board of Directors[3], outlines how cyber security and risk professionals can effectively communicate with their boards of directors about cyber security and its link to business objectives. The paper elaborated on the skills in presenting risk quantification through dashboards, illustrating metrics like key performance indicators, key control indicators and key risk indicators in categories like data loss and theft, data reliability, systems reliability, and fraud.

The NIST Cybersecurity Framework (CSF) 2.0 recommends this approach for communicating cyber risks within organisations. The CSF shows how to employ an enterprise risk management (ERM) approach to balance a portfolio of risk considerations, including cyber security, and make informed decisions. Executives receive significant input about current and planned risk activities as they integrate governance and risk strategies with results from previous uses of the CSF. The CSF helps organisations to translate the terminology for cyber security and cyber security risk management into general risk management language that executives will understand. The CSF named NISTIR 8286 as the template for this risk management integration paradigm. It is supported by four IR as analysis tools, with a focus on the prioritisation process to secure the cyber budget:

1. IR 8286A: Identifying and Estimating Cybersecurity Risk for Enterprise Risk Management
2. IR 8286B: Prioritizing Cybersecurity Risk for Enterprise Risk Management
3. IR 8286C: Staging Cybersecurity Risks for Enterprise Risk Management and Governance Oversight
4. IR 8286D: Using Business Impact Analysis to Inform Risk Prioritization and Response.

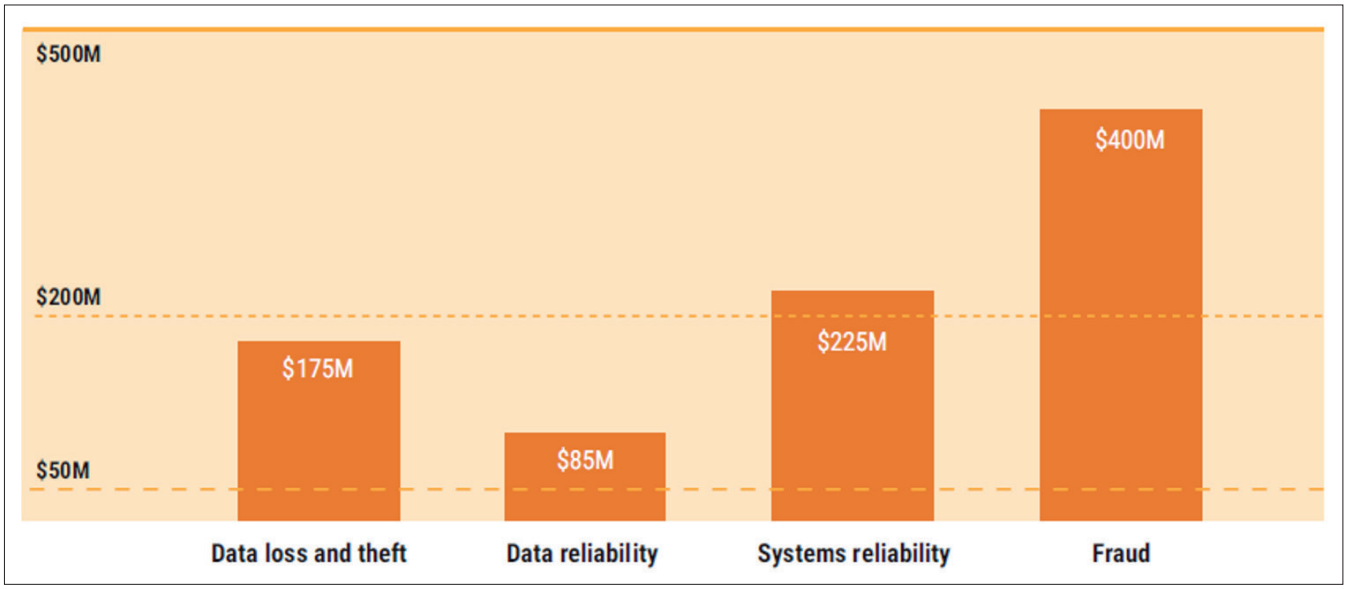


Figure 1. High-level Board Cyber Loss Report (Source: ISACA's paper, Reporting Cybersecurity Risk to the Board of Directors)

Democratising cyber risk management for women

Managing cyber risk as a business risk demands a different skill set and risk management approach. This is because security control technology without a risk context to calibrate control thresholds is limiting the effectiveness of the security protection. For example, many internal control points within business applications do not enforce multi-factor authentication, exposing critical transactions to session hijacking. Continuous authentication is increasingly mandated on high-value internal controls points, such as before committing fund transfers above defined thresholds – even for authenticated users. Generally, authenticated users are not required to reauthenticate if they are only viewing information without committing fund transfer. This balance in user experience between the effort to reauthenticate and the potential risk of unauthorised access is the essence of risk management.

Risk management, in other words, is a calculated business balance between the cost of control enforcement and a measured reduction in risks in terms of financial loss. In the previous scenario, a hijack session could be exploited to extract sensitive information, without incurring financial loss from unauthorised fund transfer, to commit other identity fraud. This mental calibration of risk demands critical thinking, empathy and listening to user feedback. Women are often considered to be more attuned to these skills and personal attributes and, therefore, are well-suited to these risk management challenges.

But, unfortunately, women are often considered to be less equipped for these risk management roles solely because of their perceived lack of technical expertise in threat analysis, malware engineering or network architecture. Since its inception in 2015, the AWSN has worked hard to debunk these perceptions and democratise cyber risk management for women, providing women at all career stages with opportunities to inspire, empower, and thrive in their professional journeys.

Its 2025 strategy is to create a voice of the industry for women, supporting the following programs:

1. Inspiring the next generation

Picture a high school student captivated by technology, but uncertain about the path ahead. AWSN has created bespoke programs – some yet to be officially launched – aimed at igniting curiosity and building essential skills. By fostering interest early, AWSN cultivates a future workforce of confident and skilled cyber security professionals ready to shape the industry.

2. Empowering women returning to their careers

Re-entering the workforce after a career break can be a daunting prospect, especially for women who paused their journeys to focus on family. AWSN offers tailored support, including upskilling opportunities, mentorship programs, and a supportive community of peers who understand the challenges. These resources provide a seamless transition, enabling women to confidently reclaim their careers.

3. Cultivating leadership excellence

AWSN prioritises empowering women to take on leadership roles in security. Through targeted leadership training, participants gain the tools, knowledge, and confidence to shatter barriers and make a

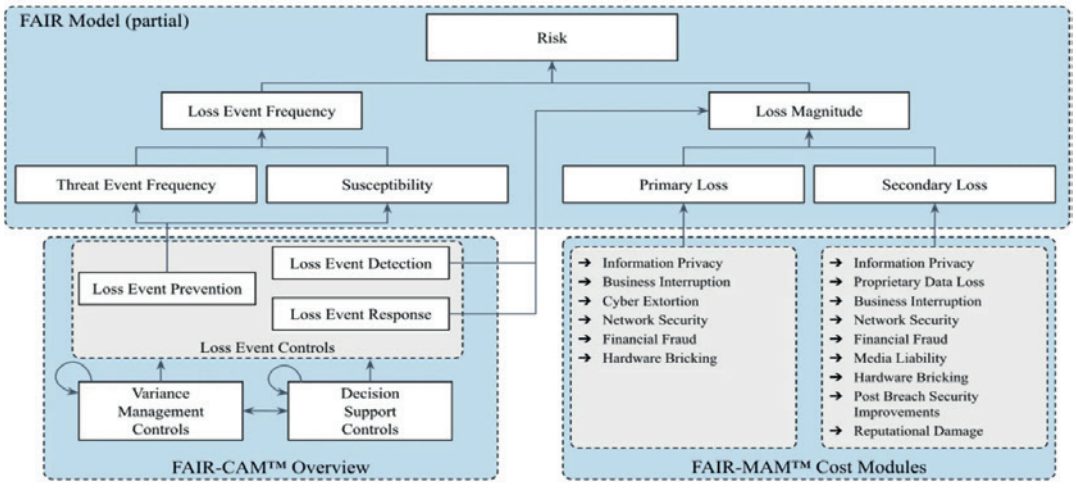


Figure 2. Integrating FAIR Models – A Unified Framework for Cyber Risk Management (Source: The FAIR Institute)

lasting impact. From managing teams to influencing organisational strategy, these women lead with purpose and inspire others to follow.

4. Strategic partnerships for growth
Collaborating with leading organisations, service providers and companies, AWSN provides unparalleled access to leadership development programs. These partnerships bridge the gap between technical expertise and executive strategy, equipping women with the skills needed to lead in boardrooms, drive critical initiatives, and shape the future of cyber security.

5. Championing women's voices in cyber security
AWSN is a powerful advocate for women in cyber security, ensuring their contributions are recognised and celebrated. By amplifying achievements, sharing stories, and driving advocacy, AWSN fosters a culture where diversity fuels innovation and progress. It's not just about inclusion; it's about leveraging every voice to strengthen the industry.

AWSN's career development programs are more than opportunities; they are transformative pathways for women – from high school students aspiring to enter the field, to experienced professionals ready to lead. Through these initiatives, AWSN continues to build a stronger, more inclusive and resilient cyber security community.

FAIR – the cyber risk business language

The CIS paper explained how to present risk quantification through dashboards. The ISACA tutorial, 'Risk Quantification 101: The Fundamentals to Getting Started'[6], explained how to apply the FAIR standard to quantify cyber risks. Unsurprisingly, NISTIR 8286 also named FAIR as the enabler for the integration of cyber security and ERM. FAIR stands for Factor Analysis of Information Risks[7], which is published and maintained by

the Open Group. The FAIR analysis process measures factors (such as threat actors and threat actions) to model the likelihood of a threat event frequency (TEF). The TEF is damped by the resistance strength of the security controls to reduce the loss event frequency (LEF). Because these factors change independently (such as different threat actors with different motivations and skills acting at different time), the Monte Carlo simulation technique is used to model the TEF and LEF to inform the design and tuning of controls. Similarly, the amount of financial loss suffered at each incident also varies independently. The FAIR standard recognises six forms of loss to calculate the total risk as the product of LEF and the loss magnitude. The CIS blog post, 'FAIR: A Framework for Revolutionizing Your Risk Analysis'[8], provides a good introduction to FAIR.

The FAIR Institute, a community of FAIR practitioners with more than 16,000 members, is driving further innovation in risk measurement to operationalise these risk insights to drive the budgeting process. The institute released the FAIR Controls Analytics Model (FAIR-CAM) and FAIR Materiality Assessment Model (FAIR-MAM) standards[9] as a unified framework for cyber risk management, as depicted in Figure 2.

FAIR-CAM examines the interdependency between controls (for example, control physiology or a system of controls). FAIR-MAM addresses the challenge of quantifying the financial impact of cyber incidents by breaking down losses into 10 modules and 26 categories, expanding from the six forms of loss in the base FAIR model.

Winning the cyber budget

Armed with risk measurement skills, women leaders are well equipped to present and defend their cyber budgets based on return on investment metrics calculated using measured reduction in financial loss, based on the expected frequency and magnitude of loss modelled on the threat environment and loss materiality. The FAIR-CAM analysis enabled pinpoint accuracy in identifying the weakest link in the chains of controls, which is the biggest contributor to the aggregate loss magnitude. This weakness could be attributed to third-party risks and/or insider threats. These insights enable the retargeting of the mitigation approach from internal technology uplift to supplier contract negotiation and fraud controls against insiders. With the support and mentoring of the AWSN communities, women leaders will have the confidence and language to win their cyber budgets. •

References

1. Mechkova, V, 'Women Leaders: Exploring the Effects of the Chief Executive Gender on Budget Composition in Comparative Perspective (2021)', Program on Governance and Local Development Working Paper No. 46, Available at SSRN: https://ssrn.com/abstract=3947097 or http://dx.doi.org/10.2139/ssrn.3947097
2. https://csrc.nist.gov/pubs/ir/8286/final
3. www.isaca.org/about-us/newsroom/press-releases/2021/tactics-for-effectively-communicating-cybersecurity-risk-to-bod-outlined-in-new-isaca-paper
4. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf
5. www.pingidentity.com/en/resources/identity-fundamentals/authentication/continuous-authentication.html
6. www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/risk-quantification-101-the-fundamentals-to-getting-started
7. www.opengroup.org/certifications/openfair
8. www.cisecurity.org/insights/blog/fair-a-framework-for-revolutionizing-your-risk-analysis
9. www.fairinstitute.org/blog/integrating-fair-models-a-unified-framework-for-cyber-risk-management

About the authors

Denny Wan *is an Australian Information Security Association Fellow recognised for his leadership and community effort in raising awareness of the Open FAIR risk quantification standard. Open FAIR, as a business language, enables effective communications between business and cyber leaders. He is a member of the FAIR Institute standards committee, tasked with driving innovation of the FAIR standards. He was named the FAIR Ambassador, recognised for his achievement in connecting business and cyber leaders to improve the communication of cyber risks. He has also been appointed as the CI-ISAC Ambassador for Risk Measurement, bringing decision science to threat-led defence, informed by risk intelligence.*

Madhuri Nandi *is a distinguished cyber security leader with nearly two decades of experience across vulnerability management, incident response, governance and risk management. As Head of Security at Nuvei, she has been instrumental in defining enterprise-level security strategies, attaining PCI compliance, and integrating advanced cloud security frameworks within the dynamic fintech sector. In her role as Co-chair on the Board of Directors at AWSN, Nandi champions diversity and inclusion in cyber security, mentoring women and fostering collaboration across the industry.*

AISA

Cyber | smart · safe · secure

aisa.org.au

cyber voices

THE OFFICIAL AISA PODCAST

Celebrating the diverse voices of the Australian cyber community.

AISA

CYBERCON 2025

AUSTRALIAN CYBER CONFERENCE

MELBOURNE | 15-17 OCTOBER

TRANSFORM TO EVOLVE

- Attend the largest cyber security conference in Australia
- Connect with over 5,000 attendees
- Engage with more than 150 exhibitors
- Hear from over 300 key innovators and experts in the industry
- Network at social events such as the Block Party, Welcome Reception, Networking Drinks, and movie night
- Participate in Locksport and CTF competitions, Careers village, book signings and Knowledge Sharing hub

REGISTER TODAY!
cyberconference.com.au