Cyber Fusion in Financial Services

How Cyber Fusion Centres are being utilised in Australian Financial services organisations

Anne Coull
College of Science and Engineering
Flinders University
Sydney, Australia
anne.coull@proton.me

Elena Sitnikova
College of Science and Engineering
Flinders University
Adelaide, Australia
elena.sitnikova@flinders.edu.au

***Abstract*—Critical infrastructure organisations with operating environments spanning multiple domains and/or with multi-dimensional threats are looking for ways to accelerate response to cyber incidents. Cyber Fusion Centres are emerging as potential models for managing inter-related multi-domain and multi-dimensional threats. Through history, military fusion centres have facilitated integrated strategic operational multi-domain situational awareness in times of conflict. The Cyber Fusion Centre has evolved from a military and antiterrorist intelligence gathering centre to become an intelligence foci for collating information and facilitating cyber incident management in organisations. Some benefit is being realised in Australia's larger banks as they manage the challenge of coordinating cyber response across disparate and siloed teams. These simple Cyber Fusion Centres provide basic, manual, reactive coordination of cyber incidents by generating open communication between response teams. But the true visionary potential of the Cyber Fusion Centre models described in the literature are not yet being achieved. These theoretical centres of response-excellence incorporating strategic threat intelligence, orchestration, crisis simulations and real-time response capability are well beyond the current reality. Analysing the original military fusion centres to fully understand how these models function, and applying this more wholistic approach to implementing fusion for cyber closes the gap between theory and practice to deliver the anticipated benefits from Cyber Fusion Centres.**

Keywords- Cyber Fusion Centre; Intelligence; Counterinsurgence Operations; Counterterrorism; Crisis Management; Continuous Performance Improvement.

I. INTRODUCTION

As the coordination centre for cyber intelligence and response within an organisation, the Cyber Fusion Centre (CFC) appears to be the logical place from whence to drive accelerated response to cyber incidents. The literature describes the CFC as a collaboration between threat intelligence, incident response, threat hunting, and vulnerability management, with the purpose of accelerating identification and response to security threats [7][10][11]. A fusion centre of this nature enables an organisation to accelerate response, removing delays by orchestrating cyber response activities that span multiple departments and teams. It allows the organisation to be more proactive in their cyber response, identifying potentially large-scale threats by collating intelligence and observations from multiple teams and systems. A centre of this nature is in a unique position to see horizontally across and vertically within each aspect of the response process, enabling end-to-end response optimisation. Ultimately, the mature CFC facilitates more proactive threat response by mitigating threats as they are identified rather than just responding after the alerts have been generated, and the incidents have occurred.

The CFC emerging in Australian banks, and documented in a whitepaper by the Financial Services Information Sharing and Analysis Center (FS-ISAC), is a simple model of collaboration between security, service management, and customer service [15]. This model is aligned with equivalent CFC capabilities operating in banks and organisations in the United States, Canada, Singapore, and Australia. Utilising fusion in this way reduces potential threat impact by decreasing time to identify complex and critical incidents and time to respond. However, the implemented CFCs have not demonstrated the degree of uplift nor the benefits anticipated in the literature.

Section II outlines the evolution of fusion centres from military coordination centres to intelligent CFCs. Section III looks at the types of CFC. Section IV highlights the uplift in capability resulting from appropriate data and technology. Section V looks at the motivating factors influencing CFC creation in Australian Critical Infrastructure (CI). Section VI assesses how CFC have been implemented in Australia. Section VII outlines the factors limiting CFC capability and Section VIII provides insight into how the gap between the theory and reality can be closed to achieve the envisioned response capability uplift. Section IX surmises the current gap between theory and practice, and the future research to monitor the evolution of CFCs.

II. CYBER FUSION EVOLUTION

Fusion centres have operated as operations response coordination centres since mankind participated in multi-domain warfare. Over time, the Fusion Centre model has evolved into a centre for intelligence, co-ordination, and

information sharing, in response to terrorist incidents and the rise of cyber-crime.

A. Military Fusion Centres

During the second world war, Winston Churchill directed the British and allied forces from the underground war room headquarters beneath London [17].

As the domains of war extended to include cyber space in the 1980s, Fusion centres have operated in the military as Joint Operations Centres, to co-ordinate operations across the multiple domains of war: land, sea, air, and space, and more recently cyberspace [2][7][13][19][23][24] (see Figure 1). Military fusion centres provided a strategic perspective of battles, facilitating coordinated information flow and driving greater efficacy in offensive and defensive operations spanning multiple regiments operating across the different locations and domains.

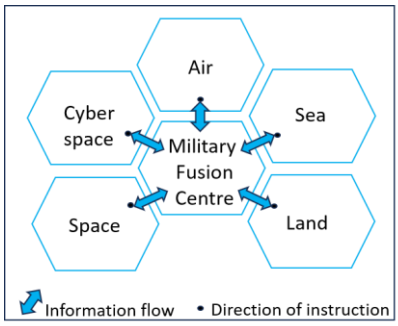

Figure 1. Military Fusion Centre model [1].

B. Counterinsurgency Operations' Intelligence Fusion and Flow

Insurgencies involve combinations of conflict and tactics across multiple domains, topographies and offensives, and counterinsurgency operations (COINOPS) need tangible real-time intelligence to stay abreast of enemy movements. This sensitivity is driven by COINOPS role working closely with civilian populations rather than conventional military forces. Counterinsurgency field commanders rely on local civilians to understand the complete geopolitical situation in which they are operating, including the insurgent actors and the motives for their behaviours. During counterinsurgency operations, this information needs to be disseminated from/to headquarters (HQ) and the field commanders in real-time. Rather than having all the intelligence capabilities centralised in military HQ, the key to the COINOPS model is to have technology and specialist personnel such as language translators and intelligence analysts, lower in the chain, implanted through all the layers from front line platoons and commanders to HQ (See Figure 2). This facilitates the flow of intelligence information, and generates greater situational transparency for the commanders at all levels. This model was demonstrated to be extremely effective in Iraq through 2006 and 2007 [19][28].

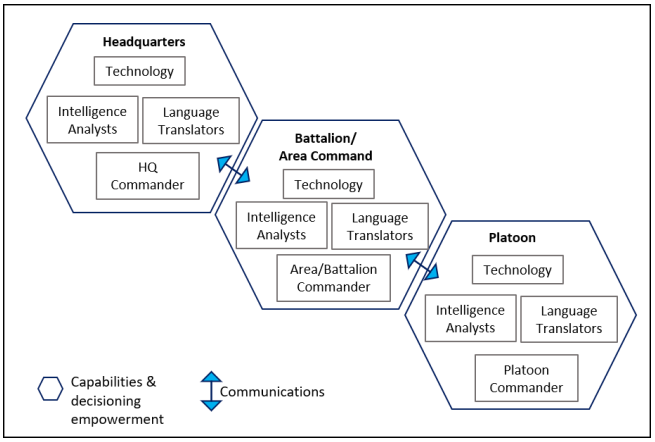

Figure 2. COINOPS model [19].

C. *Counterterrorism Intelligence Fusion Centres*

Following the New York twin tower attacks on September 11, 2001, fusion centres evolved from wartime and operational co-ordination centres into centres for collating and correlating terrorist intelligence. In the U.S.A., the Department of Homeland Security (DHS) was created at the national level, to bring together intelligence and law enforcement (See Figure 3). Correspondingly, law enforcement, public security, and emergency response were also centralised at the state level. The concept of a Fusion Process emerged, with the goal of implementing "risk-based, information-driven prevention, response, and consequence management programs" to "address immediate or emerging threat related circumstances and events" [12]. Fusion centres were created to connect the local and state intelligence centres with federal intelligence organisations and services. Aiming to prevent another successful attack on the U.S.A. through the open exchange and dissemination of analysed counterterrorism (CT) information from multiple intelligence sources [12][21][26].

This integrated model enabled more streamlined communications, collaboration, and coordination across intelligence, law enforcement and emergency response at the state and national levels, and provided actionable intelligence as the basis for security, public safety, and emergency response [26]. It was later recognised that these fusion centers also offered valuable foci "for coordinating the response to, and investigation of cyber-crimes and cyber threats against state assets and critical infrastructure. Thus emerged the Intelligent CFC [21].

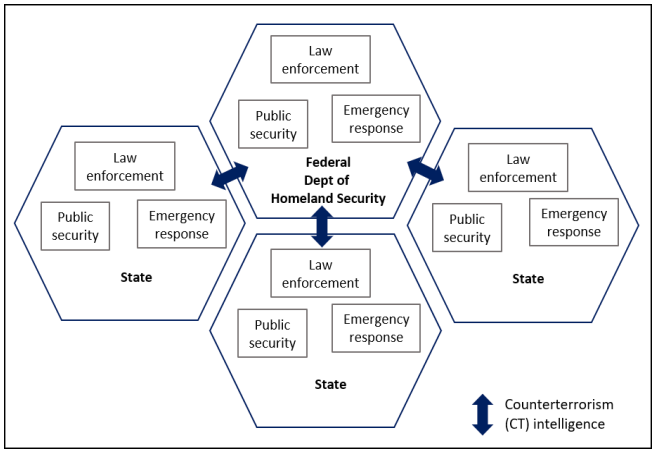

Figure 3. DHS Fusion Centre model [26].

D. Intelligent Cyber Fusion Centres

As security leaders moved from roles in military defence into business enterprises they saw the need, in their new organisations, for more efficient and effective intelligence-enabled cyber response and incident management. As a result, CFCs have been established in a number of larger organisations across the U.S.A. and in some of the larger Australian Banks, to more closely integrate cyber intelligence and operations

A CFC is described in the literature as a physical or virtual entity created through collaboration between threat intelligence, incident response, threat hunting and vulnerability management with the purpose of identifying, managing, and rapidly responding to security threats [25]. This may be a separate team, a virtual team with representation from the local response teams, or a blend, with a small group of individuals facilitating and coordinating aggregation, collation, and distribution of information across the participating teams, and analysing this integrated information to identify themes and correlations [2][8][9][26][27].

III. CYBER FUSION CENTRE THEORY

Cyber Fuson Centres (CFC) are most relevant to organisations managing multi-domain and multi-dimensional cyber threats:

a) Multi-domain

Critical infrastructure organisations, such as energy, communications and transport manage cyber threats across multiple Information Technology (IT) and operational technology (OT) domains such as: power plants, satellites, fibre networks, railway tracks and signals, etc; along with the associated networking, connectivity and access management. The operating environments in the older banks established through last century, incorporate physical and virtual technology spanning mainframes, midrange, desktops, public and private cloud, and all the associated networking, connectivity and access management.

b) Multi-dimensional

Banking and finance enterprises manage cyber threats under many guises and with many dimensions. Along with the classic external cyber threats, these organisations are also managing insider threats, fraud, money muleing, money laundering, bribery and corruption, and regulatory requirements such as sanctions and politically exposed persons (PEPs). Combatting the added layer of criminal activity in these money-motivated instances requires close co-ordination with law enforcement agencies as, in many instances, the funds are linked to crimes including extortion, drug and human trafficking, child exploitation and investment scams.

Establishing a CFC in these complex organisations, that incorporates the different cyber teams, fraud, financial crime, service management and customer experience monitoring has the potential to deliver tangible benefits:

1. Accelerated detection of multi-domain incidents such as cyber-fraud scams and website spoofing;
2. Increased accuracy, speed, and reduced cost of incident response for simple incidents such as credential compromise and malicious phishing emails;
3. Increased accuracy, speed and reduced cost of incident response for multi-domain and multi-dimensional incidents such as mule accounts, extortion, blackmail, and money laundering;
4. Early intervention on incidents before they escalate to become major;
5. More accurate reporting showing the extent of multi-domain and multi-dimensional incidents;
6. Improved ability to track and analyse trends;
7. Improved opportunity for streamlining processes and building team synergies;
8. Reduced customer impact and reputational damage with corresponding improvement in customer confidence.

In addition, when industry peer organisations work together to create cross-organisation fusion, this provides broader insights into threats, threat actor behaviours and a deeper understanding of the mitigating responses being applied, which further enhances the opportunity for response acceleration [2][7]-[11][18].

A. The Cyber-centric Fusion Centre

The literature focuses primarily around Cyber-centric Fusion Centres and describes a capability that brings together:

1. Technical Threat Intelligence such as attack vectors, suspicious domains, malware hashes, and exploited vulnerabilities to assess the cyber threats facing the organisation;
2. Strategic Threat Intelligence to map attack trends, motivations and characteristics;

3. Analysis of this intelligence to generate insights about threats and adversary behaviours, tactics, techniques and procedures (TTPs), and indicators of compromise (IOC) [2][7][8].
4. Cyber incident management [11] to co-ordinate incident response activities that span multiple teams and organisational divisions.

As it matures, the CFC described extends to incorporate:

1. Security orchestration, automation and response (SOAR), with automated operational workflows to facilitate incident triage, threat pattern analysis, and automated threat response capability;
2. Response plan testing, and crisis simulations to prepare for major incidents; and
3. Short and long-term recovery planning [7][8][26] (See Figure 4).

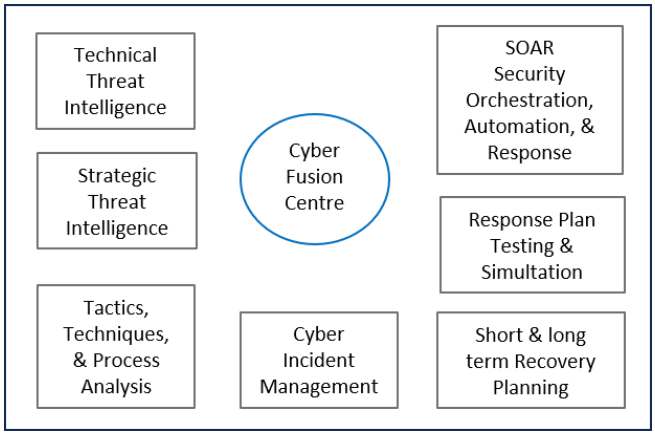

Figure 4. Intelligent Cyber Fusion Centre model [8].

B. Cyber Fusion in Financial Services

A model for Financial-services-centric CFCs has been developed by the Financial Services Information Sharing and Analysis Centre (FS-ISAC) [15]. FS-ISAC is a collaborative not for profit venture whose mission is to "advance cybersecurity and resilience in the global financial system, protecting financial institutions and the people they serve" [14]. The 2023 whitepaper released by FS-ISAC and authored by a subcommittee of its members, provided recommendations for establishing and implementing a CFC in a bank. According to the FS-ISAC whitepaper, the CFC's primary benefit is derived from sharing information during an incident, by "synchronising response activities across different regions, business units, and other fusion centers." In addition, the whitepaper highlighted that the CFC establishes a common language, streamlining communications between responders and leadership prior to and during security events, and improving c-suite risk reporting [15].

The expected benefits revolve around the resultant uplift in response capability based on:

- "Standardised, repeatable, incident response and management processes;
- Enhanced transparency into tactical reactions to events;
- Dedicated, trained, and experienced incident commanders;
- Improved adherence to regulatory disclosure requirements;
- Demonstrated overall security posture to regulators/clients/and executives" [15].

a) Fusion Centre Participants

The FS-ISAC CFCs whitepaper (2023) described a centralised, co-located or distributed, virtual model focused on response and incident management, where multiple areas in the business are impacted [15] (See Figure 5). They recommended the core participants in the fusion centre include representatives from:

- Security Operations Centre (incl. Cyber & Technology)
- Incident & Crisis Management
- Fraud Management
- Physical Security
- Intelligence
- Third Party Management
- Communications
- Legal, and Compliance.

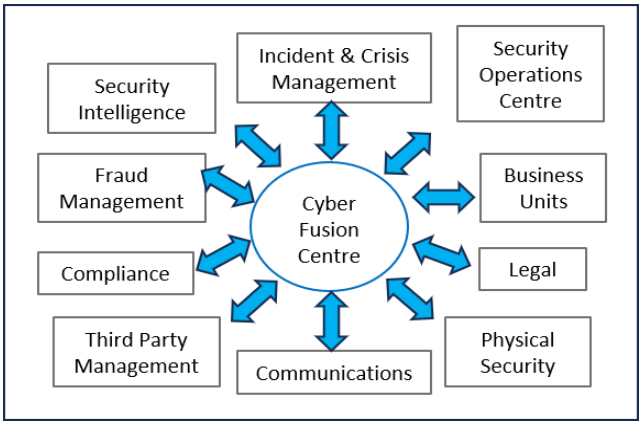

Figure 5. FS-ISAC Fusion Centre Model, based on [15].

A secondary group of participants were recommended to participate when an incident is relevant to their areas of responsibility. These secondary members include:

- Accounting
- Anti-Money Laundering (AML)
- Business Continuity
- Digital Protection & Forensics
- Data Privacy / Breach Incident Response
- Human Relations
- Group Insurance
- Internal Investigations (Insider Threat)
- Risk
- Public Relations
- Security Architecture
- Security Awareness
- Service Management (e.g., Payments, Customer Service, Internet Banking), and
- Vulnerability Management [15].

b) Implementation Model

The FS-ISAC paper outlined the method for implementing a CFC starting with a daily standup, where participants share observations and insights from the previous 24 hours. The purpose of the daily standup is to facilitate collaboration between participating teams, capture the updates they provide. Participants raise items of interest, question one another, and look for common areas of interest. The coordinating CFC team documents and tracks items raised and actions involving multiple participating teams. As the CFC matures, trends and patterns may be identified and tracked [15].

IV. FUSION ENABLING DATA & TECHNOLOGY

The strength and benefits of fusion centres comes from their ability to bring information together, in such a way that the whole is greater than the sum of the parts. Actionable intelligence comes from collating and analysing intelligence from multiple sources [25]. Fusion generates the complete threat-picture by bringing together the threat elements, or puzzle pieces [20] of techniques, tactics, and processes that only become clear when the threat is viewed from multiple perspectives. This can be achieved manually, through the standups, when participating representatives from different areas of security, fraud, service management and customer service share their observations and insights. But for accelerated fusion targeting real-time detection, supporting technology is needed. The technology platform's role is to collate the threat elements, apply pre-defined algorithms to analyse them, identify patterns and correlations, and when a defined threshold is exceeded, actionable intelligence in the form of alerts enriched with supporting information are generate, so these alerts can be actioned. Unless the alerts are analysed, filtered and prioritised, the response teams are at risk of viewing every threat as a priority, or becoming overwhelmed by the mass of alerts and missing the important ones [22][25].

Short term benefit can be realised by publishing alerts from specialist detection systems more broadly across the CFC participating teams, for example, sharing fraud and cyber-crime alerts between these respective teams.

Figure 6 illustrates the elements and interactions within the fusion enabling technology described herein. Fusion-enabling technology encompasses:

a) Data Storage

A data store, such as data lake is used to store large volumes of data from a range of sources. These may be in any format, from excel and comma delineated flat files, through to structured relational database models. Examples include intelligence feeds, vulnerability scan results, customer and employee data.

b) Utilising existing data sources

The data lake is used to bring together the data from its various sources. Existing systems will have their own data stores. Ideally, this data is ingested directly from the source system into the Fusion Data Store [DHS].

c) Intelligent Analytics Platform

In order to interrogate and analyse information from multiple sources, the Fusion Centre requires extensive analytical, discovery, and entity mapping capabilities. The scope of the analytics platform capabilities required for an organisation's fusion centre will depend on what is already available through their existing tools and platforms. As a minimum, the CFC's analytics platform needs to be capable of mapping relationships between entities sourced from multiple data sources, provide risk ratings and insights on these entities, and generate alerts where the risk rating exceeds a pre-determined threshold.

Enabling entities of interest to be discoverable will make it easier for the CFC to work with law enforcement agencies (LEA) such as the Australian Federal Police and the state level Crime Squads. Integrability, flexible data ingestion, and configurable modelling capabilities are fundamental. Additional capabilities include case management workflow, artificial intelligence and machine learning.

d) Integration

Bi-directional integration between the Analytic Platform and the data store is essential, as is integration between the data store and the source systems. Integration of the data store and/or the analytics platform with existing decisioning engines, AI tools, reporting, case management, and access management utilities will all depend on the architecture of the systems within the organisation. The platform and its capabilities will need to be in alignment with the organisation's policies and standards.

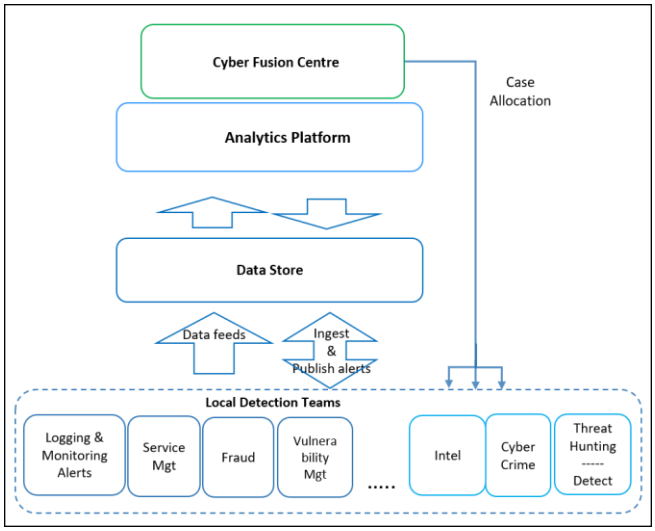

Figure 6. Fusion Enabling Technology

e) Utilising existing decision engines

Rather than recreating everything from scratch, the fusion analytics platform and data store can integrate with existing analytics capabilities. These may be machine learning tools, or AML and sanctions decisioning engines. By ingesting and publishing alerts, these analytic engines can operate collaboratively, identifying risks that only become visible by bringing information together.

f) Real-time vs Batch

Response times in cyber defence are a critical measure. Waiting overnight for a batch job will provide plenty of scope for a cyber threat actor or to move laterally through the systems domain before being found, or for a financial criminal to gain approval for a loan or credit card prior to being identified. Deeper analytics may take longer, but real-time fusion processing and risk rating is a must.

V. Motivating Factors for Establishing Cyber Fusion Centres in Australian Critical Infrastructure

The motives for implementing CFC in Australia appear to relate primarily to the scale and complexity of the organisation, perceived ease of internal communications, and the degree of scrutiny from regulators.

A. Size and Complexity Matters

Industry research indicates that only the large scale banks in Australia have implemented, or considered implementing CFCs at this time. In these large-scale organisations, the complexities of communicating between multiple teams who participate in cyber, fraud, and service management incident detection and response, with their different perspectives and priorities, has hampered fluid information flow. The large security departments that have evolved in these banks naturally segregated into silos, with each team focusing on their local accountabilities [9].

B. Smaller Scale

Smaller organisations have relied on open communications and close interpersonal relationships when coordinating their response efforts, but this is not scalable. The smaller scale organisations that were assessed in the energy and financial sectors did not see a need for a CFC, as communications and coordination during priority incidents was straightforward. Analysis found that the communications within smaller, less complex organisations, such as those within the insurance and energy sectors, is naturally more open and less arduous. With only a handful of individuals involved in incident management and cyber response, it has been easy for each participant to have a deep understanding of their own area of accountability, as well as visibility across the cyber and business landscape. In these smaller organisations, there is less opportunity for information to fall through the gaps.

C. Regulator Attention

Australian banks and financial services organisations have received close scrutiny from the regulators such as AUSTRAC and APRA for more than 2 decades. This has provided the impetus that has driven these organisations to invest in uplifting their cyber security capabilities.

The introduction of the Security of Critical Infrastructure act (SOCI), and the increased emphasis on cyber security posture across all critical infrastructure (CI) organisations reflects the shift in focus of the regulators from banks to all CI [6]. As the regulators increase the pressure across the communications, energy, transport sectors etc, there is increased motivation for these organisations to lift their cyber security capability. CFCs may emerge in these sectors as a result.

VI. Cyber Fusion Centre Implementations in Australian Critical Infrastructure

The few fusion centres in Australia are concentrated in the larger banks. These organisations are highly complex, heavily regulated, and potentially lucrative targets for threat actors and criminals [3]-[6][9]. Two large Australian Banks that have implemented CFCs were analysed. In these organisations, the CFC has played a role in bridging the gaps across disparate teams, facilitated open communications, and created an integrated perspective for cross-domain and cross-dimension response activities.

The first of the big four banks to implement a CFC established a virtual capability where people from different teams across security came together to facilitate incident response. This virtual model, while successful in achieving greater collaboration and focus in incident response was disbanded and then reformed when the Chief Information Security Officer (CISO) role changed hands.

The CFC has become more operative as it progressed through different iterations, starting with representatives from the cyber teams and evolving into a small, separate team. Along the way, it has experienced many challenges. Initially, the attendees all had day jobs so there was no-one responsible for prioritising the incidents that were identified, nor anyone assigned to capture or document them. As such, no reports were generated and the insights were only available to those present at the daily catchups. This limited the ability for others to contribute or benefit.

In addition, there were problems with managing sensitive and classified information, as the core cyber team were reticent to offer insights on situations they considered sensitive, when non-cyber participants were present. As a result, discussion became stifled, shallow, and limited, and few insights or actions emerged.

In the second Australian banks, the CFC was established with an initial focus on facilitating information flow. A new team was added alongside the detect and response teams. The fusion team coordinated daily communications forums each morning, with representatives from the different teams across cyber and physical security, fraud, IT service management priority incident response, crisis management, supplier management, and customer service (See Figure 7). Attendance included analysts through to general managers. Prior to the creation of the CFC, these specialised teams had been functioning independently, with information flow only within the core cyber teams. Coming together daily to share updates and insights with the broader group, on what they had seen in the previous 24 hours, facilitated greater transparency and visible cooperation between the teams. The CFC team was active in encouraging this cooperation, involving themselves when an incident spanned multiple domains and/or dimensions.

Beyond initial benefits elicited from the sharing of insights and improved cooperation, the value derived from the CFC has been limited. While the non-cyber teams shared their experiences openly, the core-cyber teams were slow to open up and continued to show resistance to imparting any real information. The Vulnerability Management team shared some insight into CVEs and the corresponding vulnerabilities and response actions, but the updates provided by the remaining cyber participants did not include detailed technical threat intelligence regarding the threats facing the bank, existing or missing controls, alert details, nor strategic threat intel showing trends, motivations and characteristics, and adversary behaviours. Similar to the first instance, this reticence effected the depth of discussion and the level of situational awareness across the participants, which continued to be limited and localised. Further work was needed to develop trust and a sense of shared purpose for the cyber teams.

The expected benefits from the CFC, such as accelerating threat response, were not yet being seen. The CFC had not played a role in developing SOAR capabilities, nor had they made plans to facilitate practice sessions in preparation for major or significant incidents, nor were they involved in short- and long-term recovery planning. While the CFC team supported incident management spanning multiple domains, the majority of cyber incident management continued to be accomplished locally within the specialist teams.

Despite a higher level of investment, resourcing, and visible management support, the capability and performance of this less mature CFC has been hindered by the inexperience of the CFC leader and their lack of knowledge and understanding of cybersecurity, fraud, and/or financial crime. In addition, the absence of a rousing vision for the CFC, coupled with a lack of direction and an inability to lead diverse teams and drive organisational change through inspirational leadership has stymied the CFCs ability to advance.

Without a clear vision and roadmap to propel the team forward, in this instance, the CFC operated reactively and at the task level. Continued aversion to implementing performance measures or to be involved in end-to-end process optimisation has restricted their ability to give outcome-focus their actions. This lack of strategic direction and value-add will need to be addressed if they are to demonstrate return on investment (ROI).

Neither of the bank's CFCs were enhanced with comprehensive, integrated data analytics capabilities or supported with intelligent-driven technology. The processes were mainly manual in nature, relying on regular human intervention.

Other forms of CFC were observed in different type of financial institutions. In a credit card organisation, a 2-person CFC team met with their participants monthly and focused on reviewing the events of the preceding period. The CFC summarised the events and provided a report for senior management to digest. This CFC appeared to lack the visible senior management backing they needed to drive

greater levels of participation and more active interventions, and so they had become a reporting function.

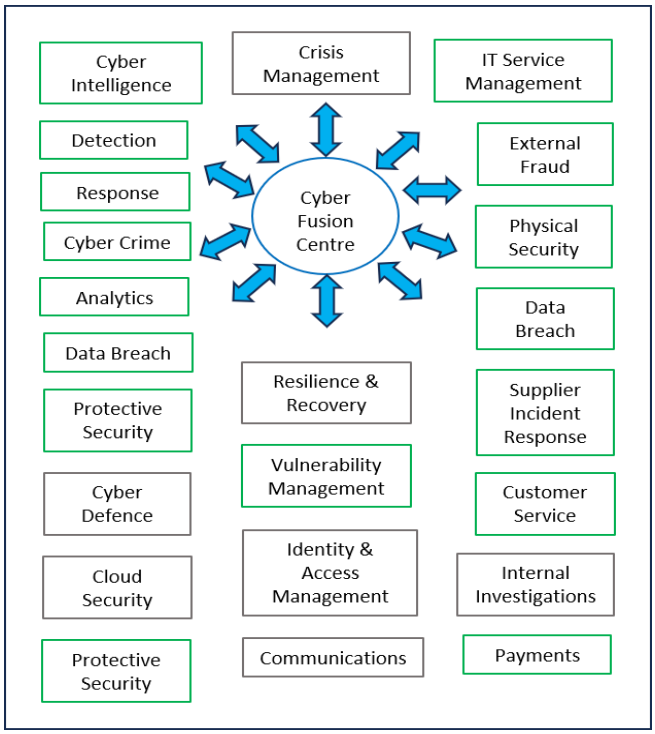

Figure 7. Cyber Fusion Centre in Australian Bank.

A. *Crisis Management*

In the Australian bank, where CFC facilitated a daily standup with representatives from across the different from the areas illustrated in Figure 7, observations were discussed, insights shared, and areas of overlap and interdependence highlighted. Where interdependencies were more complex and broader-reaching incidents were revealed, the CFC team stepped up and facilitated a more integrated response approach.

High Priority cyber incidents emerging from these collaborative sessions, whose scale of impact or potential impact exceeded an agreed threshold, were handed over to a Crisis Management Team (CMT). Crisis Management coordinated activities across IT Major Incident Management, cyber security, the affected business areas, and the internal and external communication teams. This ensured the crisis situation was prioritised, and appropriate resources were applied to accelerate recovery and minimise customer impact. It also ensured senior leadership, customer facing stakeholders and customers were aware of the outage and kept abreast of progress. The CFC team provided day-to-day support to the Crisis Management Team during a crisis situation (See Figure 8).

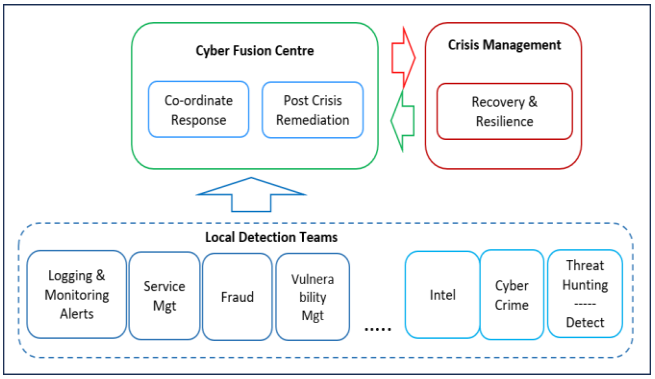

Figure 8. Fusion and Crisis Management in an Australian Bank

B. *Vulnerability Remediation*

Vulnerabilities and remediation requirements identified through this bank's Crisis Management process were captured and documented. These vulnerabilities were prioritised, funded, and remediated to ensure similar situations were not repeated. Many of these vulnerabilities had been previously reported by the accountable operations teams prior to the incident, but they had not been prioritised for funding. These larger scale incidents and the resultant crises, provided appropriate visibility and senior management focus to the potential risks, and the funding followed. The CFC was observed providing oversight and progress reporting on these remediation projects.

VII. Factors Limiting Cyber Fusion Centre Capability

The CFCs ability to influence incident response and containment times was constrained by several factors:

a) Regularity and Timeliness of Standups

The CFCs who met daily were timelier in their ability identify cross-team interdependencies, take action to intervene and thus affect response times. Those that ran weekly or monthly sessions operated primarily as a reporting and review function where events in the prior period were summarised, briefly discussed, and reported.

b) Visible Senior Sponsorship and Attendance

The priority given to the CFC, and the corresponding participation level directly correlated with the seniority and visibility of the sponsor support. Attendees joined more consistently and discussion was more open when senior leaders, such as General Managers, attended regularly, and asked questions in the CFC standup sessions.

c) Transparency, Openness and Trust

Reticence of the cyber intel teams to share details wask consistent across organisaitons. To facilitate and encourage open sharing of information and insights, the CFC need to develop a sanctum of trust amongst participants. To enable transparent and productive

discussions, they will need up-front agreement from cyber leaders that it is ok for their representatives to share specific intel information regarding threats, threat actor behaviours and impacts or potential impacts to the organisation.

d) Resourcing and Accountabilities

CFCs operated better when specific individuals were accountable for leading the CFC. These people must have adequate capacity to prioritise and follow-up on incidents, document and distribute summary reports, and perform trend analysis. This may be achieved by having separate resources allocated specifically to the CFC team, or by ensuring adequate capacity and accountability for representative cyber team members participating in the CFC.

e) Cyber Experience

The level of cyber capability of the CFC leaders and team members facilitating interactions between the participating teams directly impacted the CFCs ability to influence. CFCs led by representatives from the cyber teams themselves generated greatest participation and information sharing. Those facilitated by people with little or no cyber knowledge failed to dig into issues and performed minimal, if any, root cause analysis.

f) Follow-up Report and Actions

Those CFCs that provided a brief summary of the discussions within the catch-up session, including updates from any follow-up actions, enabled greater participation from CFC members otherwise occupied during that session. This provided greater transparency and ensured all stakeholders could stay abreast of updates and insights.

g) Data Integration and Intelligent Analytics

Technology is the ultimate enabler for bringing together from multiple sources and perspectives and overlaying real-time data modelling and analytics Without access to real-time data and enabling technologies the CFCs remained manual and under-developed.

h) *Accumulative Effect*

These factors were accumulative. The ideal results observed from daily CFC sessions being facilitated by very experienced cyber personnel, with good communications skills, participation from General Managers, visible senior sponsorship, summary reports, adequate resourcing, and follow-up actions, enabled with real-time intelligent analytics.

VIII. Realising Cyber Fusion Centres Potential: Addressing the Gap

The lack of maturity of the existing CFCs in Australia is reflected in the limited benefits they deliver. These fall far short of the goal, but the capability uplift described in the literature is attainable. The keys to addressing the gap between CFC theory and practice can be found in the fusion models that have been most successful: The COINOPS intelligence fusion and flow model, and the DHS fusion centre guidelines are readily applicable to organisations managing the risks associated with cyber and criminal activity. These models highlight the need for:

a) A Shared Vision

The COINOPS commander in the field is clear on their direction, with a strong vision of the mission objectives. The vision of a cohesive mature CFC function, that brings together every aspect of cyber: intelligence; vulnerability management; detection; response; and recovery, with technology, and customer support, for complete situational awareness, is exhilarating. The CFS vision needs to be clearly and inspiringly communicated from the top echelons of leadership through the CFC leader, to the analysts and response teams working day-to-day with the CFC [12].

b) The Right Skills and Leadership Capability

CFC effectiveness relies on the right mix of skills and capabilities, in the same way the COINOPS effectiveness relies on the right mix of skills for intelligence fusion and flow. The effective COINOPS platoon in the field incorporates both military specialists and professionals who understand the environment, with language and technology specialists, and intelligence analysts who generate situation awareness [11]. The platoon commander's understanding of the civilian and military context, in that moment, in the field, is crucial. Their depth of experience and capability is reflected in their ability to lead a diverse team of specialists, through challenging situations; distilling intelligence, providing direction; and retaining grasp of the goal while flexing to fit with the constantly changing circumstances [12][19]. The fusion centre leader requires an equivalent level of contextual appreciation, depth of leadership capability and experience, focus on outcomes, and the ability to distil information and lead diverse teams of specialists through potentially challenging situations.

c) Clear Information Flow and Accountabilities

The DHS Counterterrorism fusion model illustrates how different accountable teams can be brought together into Fusion Centres to work more collaboratively and to facilitate information flow from state to the national level [26]. The COINOPS model has taken this to the next level, accelerating the flow of

information and intelligence bi-directionally through the layers of command to enable the field commanders to make informed decisions real-time [19]. Similarly, the efficacy of Cyber Fusion and Incident Response in organisations relies on clear accountabilities along with fluid and transparent flow of intelligence information, vertically and horizontally through the organisational [12].

d) Robust Strategy and Roadmap

Turning the CFC vision into reality relies on having a roadmap that outlines the steps to get from the current, manual, reactive reality, to the proactive, informed real-time intelligent fusion analytics and integrated response capability. This roadmap needs to include all the relevant changes for policies, processes, technology and people.

e) Fusion Enabling Technology

The ultimate objectives of the CFC will only be achieved when intelligent analytics and modelling is applied across merged transaction data, alerts, and intelligence feeds from the multiple source domains. Generated insights will then highlight risks and issues not previously visible to the constituent teams.

Significant performance uplift can be attained by strategically utilising existing technology and intelligence already available within the organisation, to facilitate situational transparency and awareness across the response teams. To perform at its best as it matures, CFC will be required to leverage technology for timely information flow, integrated intelligence analytics, and orchestrated response capability [12]. Trend analysis and problem management can then be used to identify endemic issues, analyse and address the root cause(s).

f) Practice

Simulations allow processes to be refined and skills uplifted. The CFC is in an ideal position to plan and implement controlled simulations to address areas of weakness, test new process, and enhance capability and confidence in managing scaled cross-domain and cross-dimensional incidents. This capability can sit side-by-side with Crisis Management, enabling the CFC to manage incidents before they escalate to crisis level and reduce impact to customers.

g) New Ways of Working

Influencing stakeholders to overcome resistance to the new ways of working is the most challenging aspect of building a fusion centre. The CFC is a shared responsibility with potential benefits that span the business. Effective organisational change management, with visible senior-leader sponsorship, and hands-on and capable leadership from the CFC, will inspire and encourage teams to participate, learn from one-another, build mutual trust, and share in the collective gain of fusion [8][9].

h) Tuning the Model to Fit

The literature describes a CFC as a command-centre coordinating response activities, but in large complex organisations with established and experienced cyber response teams, the CFC team are facilitators, influencers, and ultimately drivers of improved response through their unique cross-silo perspective.

i) Performance Measures

Performance measures help team members to focus on the elements that make a difference. To demonstrate how the CFC can affect cyber threat response times, performance metrics such as: the Mean Time To Detect (MTTD), Mean Time To Respond (MTTR), and Mean Time To Contain (MTTC) need to be baselined and tracked [11]. Improvements in these measures will highlight the CFC's value, as well as point to areas requiring their attention.

j) Collaborative Space

Collaboration is the back bone of cyber fusion, both within the organisation, and between the CFC and other centres and cyber partners. Creating a collaborative, safe environment, where the CFC have a deep understanding of the environment and participants can openly contribute through sharing information and intelligence insights, will ensure a constant flow of information, peer to peer learning, and a continuous uplift of capabilities [12][16][25].

k) Continuous Learning and Improvement

Cyber Security, as a field, is constantly evolving: Technologies change, threat patterns change, threat actor techniques, tactics and processes constantly evolve. New vulnerabilities emerge every day with threats closely behind. The CFC is in the unique position of seeing horizontally across and vertically within the participating response teams. By working with these teams actively seeking to uplift and streamline processes, they can sustainably improve response outcomes.

l) Enduring Value and Funding

Secure adequate funding to establish, maintain, and sustain the CFC is essential for the CFCs continued existence. This will include people in the CFC, licensing costs for technology platforms and tools, technology delivery and maintenance intelligence feeds, if applicable, and more.

IX. Conclusion and Future Research

The CFC holds great promise for organisations faced with coordinating multiple divisions, departments, and domains when responding to cyber incidents. The literature paints a picture of CFCs as hubs of intelligence, knowledge, and response coordination excellence; where expertise comes together to problem solve and drive actionable

outcomes. The reality is much simpler and more basic. The CFCs described in the FS-ISAC whitepaper and being implemented in Australian banks, focus on basic manual and reactive response coordination through daily standups where representatives share their observations and insights with one another. While this has provided some benefit through great cross-team transparency, it is not delivering the anticipated improvements.

Building a mature intelligence-enabled cyber fusion capability and realising the associated benefits, requires visionary and strategic leadership, a broad appreciation of cyber security in all its aspects, an ability to engage and inspire cyber professionals to join-in, and a deep understand of the problems the fusion centre is addressing, along with the skills, technology, data, and investment to make it happen.

Future research will monitor the evolution of these CFCs, as well as other approaches and factors contributing to accelerated cyber response in critical infrastructure organisations.

REFERENCES

[1] A. Coull, "Fusion or Fantasy: Is Cyber Fusion Living up to the Dream?," Proc. CYBER 2023, pp. 38-45. Available from: https://www.thinkmind.org/library/CYBER/CYBER_2023/cyber_2023_1_70_80040.html, accessed June 2024.

[2] Anomali, "What is a Cyber Fusion Centre," Available from: https://www.anomali.com/blog/what-is-a-cyber-fusion-center, accessed July 2023.

[3] APRA, "APRA 230 Operational risk management," Available from: https://www.apra.gov.au/operational-risk-management, accessed February 2024.

[4] APRA, "APRA 234 Information Security," Available from: https://www.apra.gov.au/information-security, accessed February 2024.

[5] AUSTRAC, "New financial crime guides," Available from: https://www.austrac.gov.au/new-financial-crime-guides, accessed February 2024.

[6] CISC, "Security of Critical Infrastructure Act 2018 (SOCI)," Available from: https://www.cisc.gov.au/legislation-regulation-and-compliance/soci-act-2018, accessed February 2024.

[7] Cyware, "What is a Cyber Fusion Center Center and how is it different from Security Operations Center (SOC)?," August 2018, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/what-is-cyber-fusion-center-and-how-is-it-different-from-security-operations-center-soc-b13a, accessed May 2023.

[8] Cyware, "Building a Cyber Fusion Center, November 2020," Available from: https://cyware.com/educational-guides/cyber-fusion-and-threat-response/building-a-cyber-fusion-center-ae08/, accessed May 2023.

[9] Cyware, "Why are Financial Institutions Adopting Cyber Fusion Strategies," May 2022, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/why-are-financial-institutions-adopting-cyber-fusion-strategies-57b5, accessed May 2023.

[10] Cyware, "How Can You Improve Your Security Posture with Cyber Fusion?," June 2022, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/how-can-you-improve-your-security-posture-with-cyber-fusion-3afb, accessed May 2023.

[11] Cyware, "How Cyber Fusion Provides 360-degree Threat Visibility?," July 2020, Available from: https://cyware.com/security-guides/cyber-fusion-and-threat-response/how-cyber-fusion-provides-360-degree-threat-visibility-8fda, accessed May 2023.

[12] DHS, "Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era," U.S. Department of Homeland Security, Issued August 2006, Available from: https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/fusion_center_guidelines_law_enforcement.pdf, accessed August 2023.

[13] D. P. Fidler, "Inter arma silent leges Redu?: The law of armed conflict and cyber conflict," Cyberspace and national security threats, opportunities, and power in a virtual world, pp. 71-88. Georgetown University Press / Washington, DC 2012, Available from: https://www.jstor.org/stable/j.ctt2tt6rz, accessed June 2024.

[14] FSISAC, "Financial Services Information Sharing and Analysis Center," Available from https://www.fsisac.com/, accessed June 2023.

[15] FSISAC Fusion Council, "Considerations for Implementing a Fusion Operating Model in Financial Services– Whitepaper," Financial Services Information Sharing and Analysis Centre (FS-ISAC) May 2023. Available from https://www.fsisac.com/, accessed June 2023.

[16] Global Advisory Committee, "Cyber Integration for Fusion Centers, Global Advisory Committee (2015)," Available from: http://www.cisecurity.org/documents/CyberIntegrationforFusionCenters_000.pdf, accessed August 2023.

[17] Imperial war rooms, "Visit Churchill War Rooms," Available from: iwm.org.uk, accessed February 2024.

[18] K. L. Mclaughlin, "Cybersecurity and fusion centers," The EDP Audit, Control, And Security Newsletter 2023 Vol. 67, No. 4 2023, Available from: https://www.tandfonline.com/doi/pdf/10.1080/07366981.2023.2205689, accessed June 2023.

[19] A. Mishra, "Synchronising Counterinsurgency Ops with Effective Intelligence," Available from: https://theforge.defence.gov.au/publications/synchronising-counterinsurgency-ops-effective-intelligence, accessed July 2023.

[20] NEC, "NEC cyber fusion – actionable intelligence," NEC Corporation 2015, Available from: https://uk.nec.com/en_GB/en/global/solutions/safety/pdf/NEC_Cyber_Fusion.pdf, accessed August 2023.

[21] NGA, "Enhancing the Role of Fusion Centers in Cybersecurity," National Governors Association, 2019, Available from: https://www.nga.org/wp-content/uploads/2019/04/1507EnhancingTheRoleOfFusionCenters.pdf, accessed August 2023.

[22] A. Reeves and D. Ashenden, "Understanding decision making in security operations centres: building the case for cyber deception technology," 2023. Available from: https://www.researchgate.net/search.Search.html?query=security+operations+centre&type=publication, accessed June 2023.

[23] S. Reveron, "An introduction to National Security and Cyberspace," Cyberspace and national security threats, opportunities, and power in a virtual world, pp. 3-20. Georgetown University Press / Washington, DC 2012, Available from: https://www.jstor.org/stable/j.ctt2tt6rz, accessed June 2024.

[24] J. B. Sheldon, "Toward a theory of cyber power: Strategic purpose in peace and war," Cyberspace and national security threats, opportunities, and power in a virtual world, pp. 207-224. Georgetown University Press / Washington, DC 2012, Available from: https://www.jstor.org/stable/j.ctt2tt6rz, accessed June 2024.

[25] K. Shouse, “Actionability of cyber threat intelligence,” Utica College December 2015, Available from: https://www.proquest.com/docview/1739017603/fulltextPDF/AF5BEC7091EE448CPQ/1?accountid=10910, accessed August 2023.

[26] J. E. Steiner, “Needed: State-level, Integrated Intelligence Enterprises,” Studies in Intelligence Vol. 53, No. 3 (Extracts, September 2009), Available from: https://www.cia.gov/static/Needed-State-Level-Integrated.pdf, accessed May 2023.

[27] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A. J. Tomassetti, K. M. Repchick, S. J. Zaccaro, R. S. Dalal, and L. E. Tetrick, “Improving Cybersecurity Incident Response Team Effectiveness Using Teams-Based Research,” George Mason University, Available from: https://ieeexplore.ieee.org/document/7180274, accessed May 2024.

[28] B. West, “Counterinsurgency lessons from Iraq,” U.S.A. Army 5 May 2009, Available from: Counterinsurgency lessons from; https://www.army.mil/article/20621/counterinsurgency_lessons_from_iraq , accessed 23 February 2024.