RISK & RESILIENCE:

THE DATA OPERATIVES

FIELD GUIDE

MEMO FROM HEAD QUARTERS

Hello Partner Agent,

Cultural records show there have been two catastrophic physical attacks on M16. Both brought down critical IT infrastructure. The continuity of the organisation would have been at grave risk indeed, if not for the elite skillsets of Q Branch data operatives.

To assist you in your mission to reduce data related risk and ensure the resilience of critical information sources, the profiles of these remarkable professionals are included in your briefing pack. We encourage you to consider their roles and capabilities when forming your own mission teams.

Every partner has a choice of whether to accept the duty of guiding their alliance teams on the critical value of data resilience strategies. This is a decision you must make and execute on your own, but remember, you are never alone.

As always Crayon Headquarters is standing by and can render key services as a force multiplier for your own internal capabilities.

DATA OPERATIVES PROFILES

TECHNICIAN

The backbone of the team. Possesses expertise in data backup solutions, data encryption and automated data recovery systems. Responsible for setting up and maintaining secure backup procedures.

MASTER RECON

Field liaison. Skilled at working with allied teams to extract the information necessary to design and execute a successful mission. Provides eyes and ears on the ground to identify data assets and drive classification exercises.

> **Remember, if it hadn't been for Q Branch, you'd have been dead long ago.**
>
> – Q to Bond, Die Another Day

THE SIMULATOR

No matter the scenario, capable of simulating adverse conditions and emergency situations to test data recovery protocols. Conducts tests and drills procedure.

SECTOR PRIME

Data engineers with expertise in the unique data, file and systems used in specific industries. Works closely with Master Recons to ensure resilience strategies take all system, application, and software dependencies into account.

CIPHER

Deep encryption expert. Works closely with The Technician to ensure the most sensitive data is correctly classified and fully encrypted during backup procedures.

THE SPOTTER

Analyst trained in identifying anomalies in data and systems. Works hand in glove with peers in cybersecurity units to ensure data access privilege and identity management protocols are applied to backup data stores.

HARD CLAW

Specialises in disaster recovery plans, ensuring critical data assets can be re-established and pulled back into production environments at speed, following any event that takes them offline.

MISSION BACKGROUND

In a world where data is a critically precious commodity, the prime directive is to protect it, preserve its integrity and ensure it is always available, even in extremely adverse conditions.

There are numerous challenges to overcome. Heterogeneous IT infrastructure, data volume, growth, types and formats, lifecycle considerations, application dependencies, disparate toolsets, and regulatory conditions can make for tough terrain. You'll need to navigate complex ground to move allied companies from weak and risky data positions to strategically resilient operational environments.

Establishing your credentials and building trust will involve more than your knowledge of the common cloud platform backup fundamentals. Those in command of mission budgets may seek to confirm you are up-to-speed on their unique platform protocols.

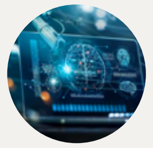
In the background there is the ever-present ticking of the clock, counting down toward an almost inevitable security event that could compromise or destroy the data you're entrusted to conserve.

Cybersecurity operatives are active on that front. But, as every data agent knows, internal and external threat actors are only part of the continuity challenge. There is no technology that can protect against the impact of extreme weather conditions, natural disaster, or unforeseen failures in the national infrastructure. The business preservation line starts and ends with you and your team.

Agents in active service should already be well versed in running standard data backup and recovery processes. This Field Guide is designed to help you establish specialist squad credentials in four industry sectors. Your ability to specialise will help you compete for mission budgets needed to advance data resilience measures into the organisations you serve.

●● **This Field Guide is designed to help you establish specialist squad credentials in four industry sectors.**

MISSION TEAMS



CEREBELLUM

K-12 Education

CADUCEUS

Primary Healthcare

MERCANTILE

Retail

FABRICATA

Manufacturing

ALL MISSION GROUND COVER

Specialised mission squads will have to train to develop the specific industry sector expertise needed to compete in the field. However, there are ground cover ops that apply in all cases.

Agents should familiarise themselves with these requirements and conduct appropriate discovery to determine if allied teams have existing measures and manoeuvres in place for the following:

1. **Data Inventory and Classification**
   Identify all data types, their sources, and their criticality to the organisation. Classify data into categories, such as sensitive, confidential, and public.

2. **Threat Identification**
   Identify potential threats to data, including external threats like cyberattacks and internal threats like data mishandling.

3. **Vulnerability Assessment**
   Assess the vulnerabilities in the data infrastructure, including weaknesses in hardware, software, and network configurations.

4. **Compliance Requirements**
   Determine the legal and regulatory requirements related to data protection and retention that apply to the organization.

5. **Risk Analysis**
   Evaluate the likelihood and impact of various threats on data. Assign risk scores to different data assets and threats.

6. **Business Impact Analysis**
   Assess the potential consequences of data loss or downtime on business operations, including financial and reputational impacts.

7. **Asset Valuation**
   Determine the value of data assets, including their replacement cost, market value, and the cost of data recovery.

8. **Security Controls Assessment**
   Evaluate the effectiveness of existing security controls, including firewalls, intrusion detection systems, and antivirus software.

9. **Access Controls Review**
   Examine who has access to critical backup pools and stores of data and who has oversight and management of controls to manage and restrict access.

10. **Backup and Recovery Assessment**
    Review existing data backup and recovery processes, including the frequency of backups, retention policies, and recovery time objectives.

11. **Resilience Levels**
    Explore extent of existing redundancy, failover systems, and disaster recovery plans.

12. **Gap Analysis**
    Identify gaps between current data protection measures and best practices or compliance requirements.

13. **Third-Party Vendor Assessment**
    Evaluate the data security practices of third-party vendors or cloud service providers engaged for data storage and processing.

14. **Incident Response Plan**
    Develop or review an incident response plan that outlines the steps to be taken in the event of a data breach or disaster.

15. **Training and Awareness**
    Assess the level of awareness and training of employees in data security and handling procedures.

16. **Regular Review and Updates**
    Frequency of assessments and reviews to keep pace as new threats emerge or as the data landscape changes.

The journey to data resilience is built on taking appropriate steps. Explore these fundamental paving stones with your allied team members, and plan what needs to be laid down to cover any gaps that could trip your specialist mission up before it begins.

MISSION CODE

CEREBELLUM

MISSION DRIVERS

Primary and secondary schools, particularly public schools often have very lean IT teams and resources. Funding is always heavily weighted into classroom outcomes. Data backup, recovery and resilience need to be given direct relevance to the objectives of school boards, administrators, and educators alike. Consider lines of inquiry that help to determine the priority settings on the following:

Educational Continuity – schools will prioritise their ability to provide uninterrupted educational services. This will include access to online learning materials, curriculum materials, lesson plans and digital resources used for teaching and learning, as well as student records. Schools may use a variety of on-premises licenses, cloud platforms and SaaS applications to deliver learning in the classroom and/or remotely. While some may be standardised, it is common for schools to provide teachers with some discretion in what is deployed. Seek to understand how many systems may be housing relevant data and files, and what the implications are for the school if these are unavailable for any period of time.

Student Privacy – sensitive data about students is collected by schools. This can include information about welfare checks, physical and mental health as well as general academic records. Access to student data should be subject to careful controls. Data classification and adherence to relevant regulatory and compliance can also be explored as part of assessing current data risk and resilience levels.

Enrolment and Registration Data – crucial for maintaining student information and academic progress records. Preservation of this data is mission critical for every school as it is often directly related to Government funding mechanisms. This may extend to data generated by Student Information Systems, which can contain student records, attendance, grades, and academic history.

> **"Securing your data is just the start....rapid recovery with no downtime and no data loss helps businesses of all sizes achieve true resilience and bounce back no matter what comes along.**
>
> – Kevin Cole, Global Director Zerto,
> a Hewlett Packard Enterprise Company

UNIQUE SYSTEM CONSIDERATIONS

Learning Management Systems

LMS are central to online and blended learning. Many schools will utilise SaaS LMS and the common misunderstandings about vendor backup and recovery of data may apply. Dig into the understanding of the shared obligation models that pertain to any LMS in use.

Remote Learning

Post-pandemic, many schools have maintained remote learning to provide better educational continuity to students that can not attend the classroom due to injury, illness, or other personal circumstance. Inquire as to the status of remote learning and if active, determine how data that is transmitted over virtual classrooms and digital collaboration platforms is factored into the overall data continuity strategy.

MISSION CODE

CADUCEUS

Primary healthcare providers such as general practice (GP) clinics often share patient data with allied health organisations such as pathologists, medical and surgical specialists, and radiology. In-clinic services can go beyond GPs themselves to include physiotherapy, psychology, and other related health services and it is useful to understand the extent to which patient data and records may be shared, as this may influence data duplication volumes for backup.

In some circumstances, practice operations may be run as shared services across multiple clinic locations, and this can influence data backup, recovery, and resilience approaches.

Medical and healthcare practices collect and store some of the most sensitive personal data imaginable. However, aside from a few highly corporatised organisations, most GP clinics are small businesses. Owners and shareholders are typically clinicians and practitioners. It is common for GPs to outsource their IT requirements, with any inhouse resources usually focused on database administration, and troubleshooting on software programs and hardware. As such, IT literacy with regards to data protection can be low, even if awareness of compliance requirements and penalty risks are clear.

Recent data breaches that hit headlines in Asia Pacific are known to have resulted in medical records of private citizens being sold on the dark web. While these attacks were targeted to large enterprise providers, smaller practices are soft targets. Beyond the risk of data being stolen or ransomed, downtime to core systems can result in lost bookings and impact to revenues.

MISSION DRIVERS

There is a common misconception that GP practices have healthy budgets because it is generally accepted that Doctors do well financially. In truth, doctors may take home good earnings, but this does not mean their practice operations receive adequate funding. It is common for the practice itself to only receive 10-12% of all revenues, and this is where the budgets for all operational requirements are drawn, including technology investments, licences, and services.

In practices where there is a shared services model, it is more likely to find a General Manager or CEO with broader business knowledge and better appreciation for the value of investing in data backup, recovery, and resilience strategies. However, consider for the most part that decision makers will be non-technical. This means making your mission relevant to what they value most:

Patient Care Continuity – Availability of medical records is mission critical. GPs cannot accurately diagnose, treat or prescribe to patients without consulting them. Explore the implications if core systems and data availability is offline for any length of time.

Reducing Compliance Burden – the cost of regulatory compliance is a heavy burden for practices. Aside from government regulations, many practices also have to contend with a host of process compliance associated to medical insurance claims. There is a lot of data required, which is often scattered across multiple systems and often has to be retained for long periods of time. In the event of data loss or unavailability, it can affect the ability of practices to lodge claims and receive payments, which can directly affect cashflow.

Appointment Scheduling – Some clinics will use a SaaS provider with open APIs. Others may have legacy systems or may rely on basic processes such as spreadsheets or shared calendars. It is worth discussing how appointments are scheduled, how the relevant processes and data are managed and what the implications are when Drs lose visibility over their appointments for any length of time.

UNIQUE SYSTEM CONSIDERATIONS

Telemedicine/Telehealth

Much like schools, some GP clinics will have launched remote service offerings during the COVID pandemic and may still have these in use for patients that are unable to get to a clinic setting. It is possible that some practices implemented their telemedicine or telehealth offerings very quickly as the pandemic unfolded, and this can result in a lack of data integration or gaps in the data backup and recovery processes. Services may be provided via voice and/or video link, so it is useful to inquire as to how relevant data is handled and what the retention requirements may be.

Clinical Information Systems

These systems store electronic health records and patient data. It is common for markets to be dominated by a small number of incumbent vendors, and as such modernisation from proprietary ISV offerings to full SaaS solutions has been slow. This can make data integrations challenging for small GP clinics, which do not have inhouse expertise to support their data strategies and executions.

ePrescribing Systems

Electronic prescribing solutions facilitate the ordering and dispensing of medicines and pharmaceuticals, by transmitting the prescription details directly from the GP to the patients preferred chemist outlet. Platforms for ePrescriptions may be mandated by Government, depending on country. Up until COVID, these systems and platforms were in place but not widely used. Demand exploded through the pandemic, and patients have now become used to the convenience this provides. It is worth inquiring about the current use and expressing interest in how and where data shared between GPs and chemists/pharmacies is backed up.

Booking Engines

There are often a small number of incumbent vendors that hold large market share for medical booking engines. As a result, some have not transitioned to full SaaS and this can result in challenges with data integration, which in turn can have implications for backup and recovery. When these engines go down, it can have a material impact on revenues and lead to a spike in costs, as GPs need to put on additional staff to cover higher volumes of inbound calls. Explore what the arrangements with the vendors are for backup and recovery in the event of engine failure or data compromise.

MISSION CODE

MERCANTILE

The retail sector across Asia Pacific has bounced back somewhat from the pandemic battering. Headwinds still remain; operational costs continue to rise for retail rental, customer acquisition, supply chain, logistics and running online business models, but consumer spending confidence is still volatile. Retailers invested heavily in technology to adapt to the pandemic conditions and are likely to be carefully assessing the return on investment. Data operatives will need to address how data backup, recovery and resilience will contribute to increased business value.

MISSION DRIVERS

Customer Experience: Technology-driven customer experiences such as online shopping, click-and-collect and personalised recommendations rely on data. A recent Forrester study of APAC SMBs showed improved Customer Experience to be one of the top four strategic priorities for SMBs across the region. Connect the data resilience mission to the CX priority to gain traction in your discussions.

Data Security and Compliance: ensuring the security and integrity of customer and transaction data is paramount for retailers. Compliance with data protection regulations and standards such as GDPR and PCI DSS drives investments, as security is now understood by retailers to be a core trust pillar in maintaining customer confidence and protecting reputation. Retailers are targeted heavily by threat actors because of the PII they collect, and the large volumes of financial transactions made across systems. Data breaches and operational disruptions can severely damage reputations and erode the ability for SMB retailers to effectively compete.

Explore whether the rapid adoption of eCommerce platforms and SaaS applications during the pandemic may have left gaps in data protection frameworks, and attach your resilience mission to competitiveness, customer trust and loyalty outcomes.

Revenue protection: System downtime and/or the loss of transaction data has severe implications for retailers. The most immediate impact is financial. Every second that Point-of-Sale systems or eCommerce platforms are down costs money. Unrecoverable transaction data results in losing the value of the transactions. It also disrupts inventory management and can lead to overstock or stockouts, both of which have an impact on the bottom line. Provide mission case studies that prove streamlined backup, recovery and resilience strategies can prevent or mitigate system downtime and data loss. Connect the dots back to revenue protection.

Vendor and Partner Relationships: Retailers that stock products from well known brands may be subject to proving they have appropriate data protection and resilience measures in place. As large brands seek to sure up supply chain security and resilience, trade agreements may include serious penalties for retailers that commit to such terms but fail to execute on their end of the agreement. Do your reconnaissance on the brand items that are stocked in your target retail outlet. Check the brand company website and/or annual reports for any specifics on their data protection policy statements and commitments. This can prove an interesting and compelling talking point that demonstrates you have the finger on the pulse of influencing forces in retail operations.

> **Controls used to monitor access to on-premise backups do not always translate one-to-one to cloud-based systems. Designing a cloud-based solution, organizations need to consider how access is controlled, how requests to retrieve or store data are authenticated and how the backup live cycle from creation over retrieval to eventual deletion is managed.**
>
> — Dr. Johannes Ullrich, Dean of Research at SANS Technology Institute

UNIQUE SYSTEM CONSIDERATIONS

POS, eCommerce/ mCommerce Platforms

With the growth of online shopping, retailers often have diverse transaction data sources to contend with. Transaction data may be collected instore, online and via mobile payment applications. eCommerce platforms often require real-time data synchronisation, and this means the backup strategy has to allow for capture of data changes as they occur. This data is often used to provide insights to consumer buying trends, which in turn feed decisions around inventory management, stock orders, shipment, and fulfillment. Integrating data from different sources into a unified backup system can be challenging, especially when data structures, formats and protocols vary. The unique, specialised skills of data operatives familiar with retail operations can guide retailers on how to achieve this goal, avoid data inconsistencies and duplications that can lead to errors in customer orders, forecasting and reporting.

Supply Chain and Logistics Solutions

Managing the movement of goods from suppliers to retail stores can be burdensome for SMB retailers, especially if they are utilising manual or legacy systems. The value of Enterprise Resource Planning solutions is well documented on this front, but the backup and recovery of enterprise application data can present unique challenges. Be sure to run discovery into this part of the retail operation, and discuss where this critical data resides, how it is protected and what the implications are if there is disruption, downtime, or loss. Talk to your customer about how they can leverage single platform options that can combine the productivity suites they probably already use with ERP solutions from the same vendor. Help them to understand the advantages this can bring to ensuring streamlined data backup and recovery, and how it can support greater data resilience overall.

MISSION CODE

FABRIKATA

SMB manufacturers are by nature, efficiency driven operations. There is pressure to control production costs and carefully manage margins to be profitable.

Many manufacturers, even small, boutique and family run operations are often working with highly sensitive information. Proprietary designs, production methods and customer data need to be given proper protections. Equally, manufacturers may also be working with unique data types and formats, particularly if they utilise 3D printing or Computer Aided Design (CAD) and Computer Aided Manufacturing (CAM applications such as Autodesk.

There has been a lot of disruption of manufacturing across Asia Pacific. As the implications of the volume of world production managed through manufacturing facilities in China became apparent during the pandemic, many brands have sought to diversify their manufacturing and production lines into neighbouring countries such as Thailand and Vietnam. This is driving increased modernisation in emerging economies, and data management frameworks will need to keep pace. In some instances, manufacturers may need to demonstrate they can match the data protection requirements of international customers, and this is an opportunity for your Data Operatives to provide much needed guidance.

MISSION DRIVERS

Production Downtime: Seek to understand the direct impact of data loss and system downtime on manufacturing operations. Disruptions that lead to production delays can have an immediate impact on revenues and contractual agreements. SMB manufacturers have to work hard to compete for their business. Show them how running a tight ship on data backup, recovery and resilience can support their ability to compete and protect their production line capacity.

Quality Control Data: Core systems in manufacturing environments often produce data that is used to monitor and measure production quality, product specifications and compliance. Manufacturing relies heavily on consistent product quality. If this data is unavailable or lost, it can hold up production or result in inferior outputs. Explore where and how quality control data is captured, and if there is any risk to the backup and recovery process.

Product Traceability: Manufactured products will often be produced subject to recalls and warranty claims. Traceability data needs to be protected and readily accessible in the event of an issue with batch productions or in case of a general recall due to quality, safety or other issues. Your Data Operatives may not have particular skillsets or solutions that apply to this unique requirement. Nonetheless, asking about whether a manufacturing customer needs and uses traceability data helps to establish your understanding of the sector, and builds additional credibility for your team.

> **As with all platforms, the protection of data is critical to business. The key area of focus for me though is making people aware and to understand the importance of data backup when it comes to cloud and cloud native. As many businesses are in process of moving their workloads into the public cloud and consuming as a service, it's important to note that this doesn't remove the requirement for data management. The cloud providers are going to keep the infrastructure available and resilient, but the data is on you as a company.**
>
> – Michael Cade, Field CTO of Cloud Native at Kasten by Veeam

UNIQUE SYSTEM CONSIDERATIONS

SCADA and Industrial Control Systems

Manufacturing often relies on Supervisory Control and Data Acquisition (SCADA) and ICS. These systems are computer based and are used to monitor and control various process and operations. SCADA systems collect data from sensors, instruments and devices in real-time. They provide real-time visualisation and monitoring of collected data through GUIs and allow operators to control various processes and connected equipment remotely. As such they are mission critical to manufacturing operations. Enquire about the use of SCADA, and ensure your Data Operatives understand the data dependencies, and how SCADA data sets are connected through the entire manufacturing operation.

Shop Floor Connectivity

This relates to SCADA but can also incorporate other data sets that are generated by manufacturing systems and applications. Resilience network infrastructure is key to manufacturers, as it ensures real-time data capture, monitoring and control of their processes. Understanding the network within the manufacturing environment can help to identify risks, limitations and opportunities for the data backup and recovery mission.

CULTURE IS KEY TO THE MISSION

Addressing the human element is critical to the success of the Data Resilience mission. Poor organisational culture will eat you r Data Protection strategy for breakfast. When running reconnaissance into allied operations, keep a careful watch out for indicators of both poor and healthy behavioural traits, as each provide vital insights into how you will need to guide your customers to safe ground.

RISKY CULTURE INDICATORS

Data Neglect: Employees show little interest in or concern for data security and resilience, often neglecting data backup procedures.

Lack of Training: The organisation doesn't invest in data security and resilience training, leaving employees unaware of best practices.

Blame and Cover-Up: When data incidents occur, employees may try to cover up mistakes or shift blame, hindering open communication about data issues.

Low Compliance: Employees consistently ignore data security policies and best practices, making the organisation vulnerable to data breaches.

Resistance to Change: The organisation faces resistance from employees when implementing new data resilience strategies or technologies.

Silos and Lack of Collaboration: Departments work in isolation, hindering effective data sharing and cross-functional collaboration in data recovery efforts.

HEALTHY CULTURE INDICATORS

Data Ownership: Employees understand the importance of data as an asset and take ownership of data security and resilience.

Continuous Training: The organization invests in ongoing training and awareness programs to educate employees about data best practices and security protocols.

Transparency and Accountability: Employees are encouraged to report data incidents, and the organisation fosters a culture of transparency and accountability when addressing data issues.

High Compliance: Employees consistently follow data security policies and best practices, reducing the risk of data breaches.

Adaptability and Innovation: Employees embrace new data resilience strategies and technologies, adapting to changes in data protection practices.

Collaboration and Communication: The organization encourages open communication and collaboration among teams, facilitating efficient data sharing and collective efforts during data recovery.

RESILIENCE IS THE MAIN CHARACTER

The best Data Operatives are masters of the protective arts. They use technical intellect and skillsets rather than roundhouse kicks and jujitsu blows, but their actions carry just as much weight in the defensive strategies of their customer organisations.

What gives you and your customers the edge is resilience. Carrying through with the Data Resilience mission is about giving your customers the ability to bounce back quickly from the unexpected knocks to operating conditions.

It's the data equivalent of fighting off multiple assailants with a pen, then speeding down a ski slope, avoiding machine gun fire and finally rescuing everyone from the bowels of a burning building. Resilience allows highly trained data operatives and their customers to get up every day, and do it again and again with increasing success.

Resilience is learned, rather than earned, and usually as a result of experience gained on multiple missions. Every deployment into the field builds a stronger, faster and ever more adaptable organisation.

WE WISH YOU EVERY SUCCESS IN YOUR MISSION.

To discuss the parameters of your journey, request a meeting with our Technology Advisory Team, they are on standby to help you.

TAG.bc@crayon.com

Crayon