Deloitte.

Superannuation

Rich Opportunity for Cyber Criminals?

November 2018

Over the past decade, cyber crime has affected financial institutions and their consumers with increasing sophistication, frequency and impact. Large account balances, low member engagement and low cyber maturity makes the superannuation (super) industry an attractive outlier for cyber criminals, leading to a growing cyber crime challenge for the industry.

On a regular basis the phone rings at Deloitte Cyber HQ for us to respond to a client that has had a cyber incident. Our response team duly grabs their packed bags to head out to the client site and begin the process of investigation. Over the years, the nature of these responses has changed. In the early years, breaches were occasional and tended to be singular incidents of data theft. In recent years however, we've noticed a significant rise in incidents where a cyber event has then led to the client's own staff being manipulated or coerced to make a fraudulent payment.

We are not alone in noticing this trend of cyber attacks converging into financial crime. In July 2018, the US Federal Bureau of Investigation (FBI) stated that global losses from one type of cyber crime (business email compromise) had exceeded $12.5bln.[1] This type of crime uses email as the primary vehicle to coerce or convince individuals to perform unauthorised transfers of funds. It has been particularly prevalent in the real estate and conveyancing industries, exploiting the widespread use of email for exchanging beneficiary accounts and changing the settlement account at the last minute.

A second example of this growth is the cyber-enabled attacks on banks that use the SWIFT[2] network, including one example where an Asian central bank suffered a financial loss of over $80 million. In these attacks, criminals used a combination of cyber techniques and detailed domain knowledge of SWIFT to inititate payments and divert the funds to other jurisdictions, where funds where withdrawn. A large proportion of the money taken in these attacks may be unrecoverable.[3]

What makes super funds an attractive prospect for cyber criminals?

Superannuation is an attractive outlier. In the APRA Cyber Security Survey[4] of all financial services entities, the super industry was highlighted as having the highest frequency of material cyber incidents, with 75% of respondents having incidents that required escalation to executive management. The industry also had the lowest level of preparedness for an incident.

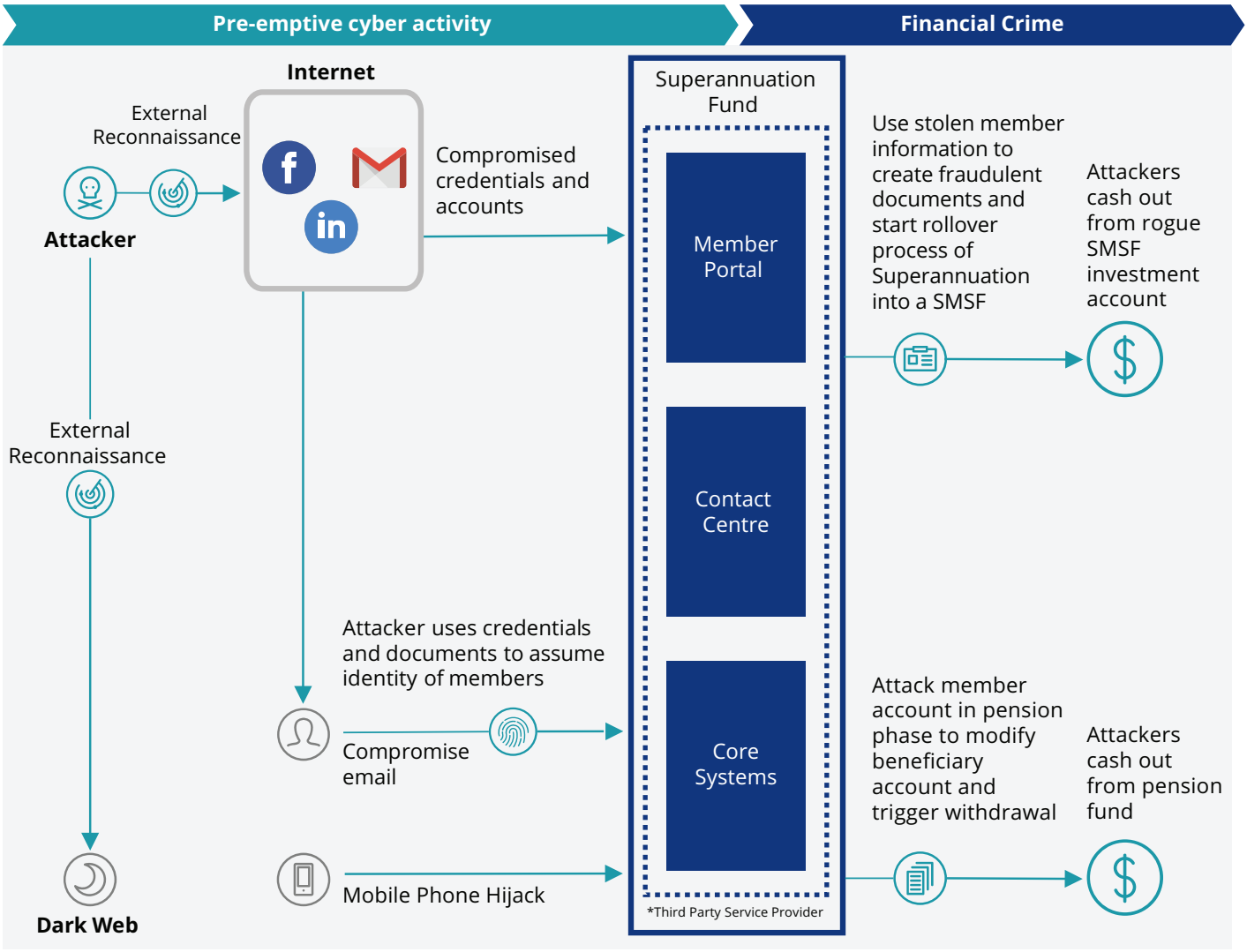
A number of unique characteristics explain why the industry is becoming an attractive target for cybercrime:

- **Oversized money pools.** Australia has the world's fourth-largest superannuation market[5], with assets over $2.7 trillion, and an average growth rate of 7.9% for the period 2017-18.[6]
- **Low member engagement.** In general, members infrequently check their superannuation accounts or read the statement.[7] This can significantly increase the period of time between a successful fraud event (e.g. withdrawal or rollover) and the detection of that event by the member.[8]
- **A complex third-party environment.** As a whole, the industry has a high reliance upon third-parties such as administrators, financial planners and other outsourced providers who perform services or engage with members on their behalf.[9] This increases the range of potential attack points cyber criminals can target and commit fraud, without the fund itself directly having visibility.
- **Improving member experience is a point of differentiation.** The industry is rapidly improving the functionality of online member portals and mobile apps, so that members can interact and perform transactions from a range of devices on a 24x7 basis. This is in turn increasing the inherent risk that an attacker can access member information or initiate transactions if they have the member's log-in details.[10]
- **Faster payments.** Technology adoption and regulations such as SuperStream are driving a transformation of the superannuation industry towards a fully interconnected environment with faster velocities on withdrawals and rollovers. These faster velocities can mean that outbound payments or rollovers are made promptly, with limited human oversight, and can reduce the time window for detection of a fraud or recovery of funds paid in error.

How a cyber attack can lead to fraud in super

Deloitte often works with clients to perform risk assessments based on real-world attack scenarios that imitate how real cybercriminals operate to compromise a fund. We find these are particularly effective at explaining the convergent nature of the threat and to then help clients design layered controls that map to the stages of attack.

The diagram below highlights a common attack scenario, which demonstrates the two main phases of cyber activity followed by the actual financial crime. In general, the aim in the cyber stage is to acquire enough personal information and access on behalf of a member to then overcome the controls that govern a rollover or withdrawal process.



Finding breadcrumbs of information. The first stage involves cyber criminals conducting online reconnaissance across both the indexed internet and the dark web to find 'breadcrumbs' of information from external data sources about members. A common goal is to identify stolen username and password combinations (thanks to major breaches over the past five years there are more than five billion combinations now available online), which can often be tried against other websites that the individual uses, such as the super member portal or personal email account. This technique is made more effective because passwords are widely reused between websites – the average individual has more than 100 online accounts protected by five passwords or less (and 23% of individuals use the same password for all their accounts). The attackers may also combine this activity with relatively simple information gathering techniques to find information (e.g. date-of-birth) from open sources such as social networks like Facebook.

Personal email account takeover. Attackers will also employ techniques like 'phishing' to attempt takeover of the personal email account of a member. In our experience, this technique is a particularly effective staging point because these accounts often yield a wide variety of 'useful' information to conduct fraud, such as high-quality copies of signatures (from scanned documents in the Sent Items folder), Tax File Numbers, date of birth, full names, and previously signed superannuation forms.[11]

Compromising the member portal. The average personal email account is now associated with more than 100 other online accounts. This means that if the member uses their personal email account for their super member account registration, then attackers with access to the account can then trigger the password reset process on a member portal and capture the reset email, enabling them to log-in as the user.

Mobile phone hijacking. A number of super funds have adopted multi-factor authentication which relies upon a text message being sent to the member at the point of log-in, or to authorise higher risk transactions. Unfortunately, this has triggered a corresponding growth in mobile phone number theft, whereby the attackers can use relatively simple personal information to maliciously port the members mobile phone number (within about 15 minutes) to a prepaid SIM for long enough to be able to access the portal.[12]

Executing payment fraud. Once attackers have access to sufficient information about a member, cyber criminals can then directly attempt fraud using the documents, information and keys collected. Common fraud scenarios might include submitting false information to trigger a SMSF rollover or withdrawal request (of an account in the pension phase) into a bank account that is controlled by the criminals.[13]

Detection can be slow. Distinguishing normal withdrawals and rollovers from malicious activity is extremely challenging for superannuation funds. It is common that the first red flag is the point at which the member checks their account or receives a letter in the mail to advise them of the transaction. Additionally, superannuation funds that outsource operational matters to third-party service providers may have a lack of clear arrangements regarding fraud monitoring and reporting requirements, making the detection of criminal activity increasingly difficult.[14]

Why passwords are a failing control

59%
of individuals have five or fewer passwords, yet have an average of over 120 online accounts.

23%
of individuals always use the same password for all websites.

56%
of employees reuse passwords across personal and corporate accounts.

The average personal email address is registered with over **100** online accounts.

There are over **5 billion** username and password combinations exposed by data breaches.

Personal email accounts hold the key to the lives of members and are a staging post for attacks

Accounts typically contain a wide range of:

- Identification documents
- Personal information
- Contracts containing high-quality scanned signatures.

Once compromised, the personal email account can be used to intercept password resets on most accounts.

Convergence of cyber monitoring and forensic analysis

An inherent challenge to successfully joining the dots to discover that a cyber-enabled fraud event is occurring is the current siloed nature of data in organisations.

For example, if a cyber criminal posing as a fund member happens to a) trigger a password reset on the member portal; b) ports their mobile phone number to a new carrier; c) logs into the member portal from a new location using a new device; d) updates their beneficiary account for withdrawals and e) requests a withdrawal – the super fund needs to have visibility and insight across a range of data sets and the capability to successfully join the dots to identify that a fraud could be occurring (and in time to take action).

Hence, a further step in the journey of mitigating the converged risk involves combining cyber and transactional data sets across the business to look for unusual patterns that may indicate a progressive multi-stage attack is occurring to assist decisions around payments. This combined dataset is essential to determine the overall financial impact, and to inform effective customer experience management efforts.

So what analytics capabilities should be considered?

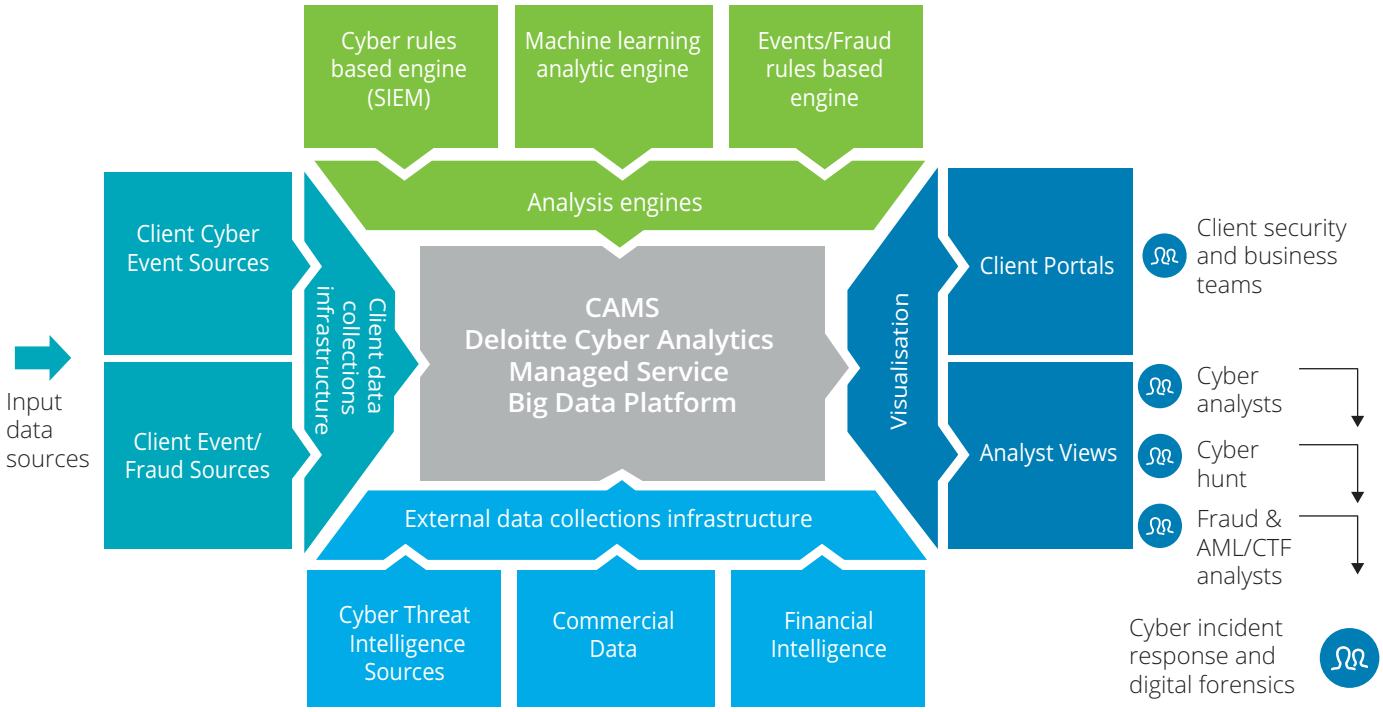
Deloitte employs a wide range of analytic techniques for the quantification of overall transaction risk using a converged range of data sources, and to provide a landscape view that will facilitate the proactive management of cyber risks.

There are four steps to this process:

1. **Authentication Analysis:** Suspicious markers on customer events will allow for the identification of at-risk accounts.
2. **Analytic Testing Procedures:** Typologies are developed to identify known patterns of behaviour highly correlated to fraudulent redemption events.
3. **Transaction Risk Scoring:** Transactions are scored based on features of the redemption to identify likely fraudulent redemptions outside of what had been self-reported.
4. **Customer Behaviour Analysis:** Transactions are then put in the context of a customer's typical behaviour to further inform the quantification of likely customer financial impact.

Deloitte has developed a Cyber Analytics Managed Service (CAMS) to combat cyber-enabled fraud in super and provide deep insights into member behaviours that can help identify transactions that are worthy of further investigation. The heart of this system is a big data platform enabled with machine learning to detect both known and unknown events attributable to fraudulent or suspect behaviours.

The following diagram provides an illustration of our approach.



Raising the bar

The multi-stage nature of cyberattacks means that super funds and administrators need to consider a risk management approach that directly maps mitigation techniques to each stage of the attack scenarios – and also ensure they can join the dots between stages.

Five key areas that organisations in the superannuation industry should consider are:

1. **Perform cyber risk assessment based on real-world scenarios:** Cyber risk assessments should be based on a set of realistic attack scenario pathways that are based on how cyber criminals actually seek to attack the fund (or the third-party landscape).[15]

2. **Threat intelligence:** External threat intelligence can help monitor both the public Internet and the dark web to identify emerging cyber threats and attack groups that are currently targeting super funds and their members. Moreover, this capability can also be used to identify compromised usernames/passwords and correlate this against the current passwords of members that use the member portal – which can be used for proactive outreach to members (e.g. to choose a stronger password).

3. **Human Resilience:** A significant number of cybercrime events still involve some degree of coercion of staff, third-parties or members. Modern organisations are developing role-based cyber risk assessments and learning needs analysis to develop targeted training that is specific to the risks associated with each role and includes practical examples.

4. **Effective cyber detection:** In a significant number of cyber breaches, there is an extended period of time between the initial infiltration and the risk event. However, most organisations have millions of security log events, which presents an extreme 'needle in the haystack' scenario. Mature organisations are investing in sophisticated detection capability, which includes skilled analysts, and detection use-cases/ behavioural analytics that are mapped to the specific financial crime risks.

5. **Incident and crisis response:** An increasing reality is that organisations experience malicious significant cyber events on a recurring basis. Significant events often put pressure on an organisation to make effective decisions under time pressure, and recent regulatory reform means that organisations are sometimes expected to perform outreach to thousands of impacted individuals. For these reasons, it's particularly important that the incident and breach response process is well defined and practiced to the point where there is familiarity across the whole organisation.

Contacts

David Owen
Partner
Risk Advisory
Sydney
E. dowen@deloitte.com.au

Simon Crisp
Director
Risk Analytics
Sydney
E. simoncrisp@deloitte.com.au

Greg Janky
Partner
Risk Advisory
Melbourne
E. gjanky@deloitte.com.au

Puneet Kukreja
Partner
Risk Advisory
Melbourne
E. pkukreja@deloitte.com.au

Endnotes

1. https://www.ic3.gov/media/2018/180712.aspx
2. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardised and reliable environment.
3. https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH
4. https://www.apra.gov.au/sites/default/files/Information-Paper-Cyber-Security-2016-v4.pdf
5. https://www.austrade.gov.au/news/economic-analysis/australias-us1-6trillion-pension-superannuation-system-is-the-fourth-largest-in-the-world
6. https://www.superannuation.asn.au/resources/superannuation-statistics
7. https://www.ato.gov.au/Media-centre/Media-releases/New-statistics-reveal-$14-billion-in-lost-super/
8. http://austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB.pdf
9. http://austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB.pdf
10. http://austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB.pdf
11. https://www.forbes.com/sites/forbescoachescouncil/2017/12/21/account-takeover-attacks-are-on-the-rise-and-you-need-to-hear-about-it/#4b3e3ec565d1

12 https://www.bankinfosecurity.com/gone-in-15-minutes-australias-phone-number-theft-problem-a-11552

13. https://www.moneysmart.gov.au/scams/superannuation-scams
14. http://austrac.gov.au/sites/default/files/super-annuation-risk-assessment-WEB.pdf
15. https://www2.deloitte.com/content/dam/Deloitte/au/Documents/financial-services/deloitte-au-fs-superannuation-industry-connectivity-transformation-220818.pdf

Deloitte.