

Unbroken chains - DBIR 2019 Report

**Profiling organisation - FAIR Analysis**

By [Denny Wan](https://www.linkedin.com/in/wandenny/), peer reviewed by [Gabriel Bassett](https://www.linkedin.com/in/gabriel-bassett/) and [Wade Baker](https://www.linkedin.com/in/drwadebaker/)

The [Open Group FAIR](https://www.fairinstitute.org/what-is-fair) cyber risk quantification framework aims to create a common risk language that all can understand across an organisation. A common understanding is essential for [targeting cyber security investments](https://www.fairinstitute.org/blog/targeting-cybersecurity-investment-the-fair-approach). This article explains how to use real-world breach data from the [VERIS Community database](http://veriscommunity.net/vcdb.html) and [Verizon Data Breach Investigations Report](https://enterprise.verizon.com/resources/reports/dbir/) (DBIR) to model organisation risk profile to be used in the FAIR analysis.

The six-phase FAIR analysis process begins with a realistic modelling of the risk scenario:



Figure 1: 6 phases of the FAIR analysis process. Source: The FAIR book

The [Verizon Data Breach Investigations Report](https://enterprise.verizon.com/resources/reports/dbir/) (DBIR) provides a fact-based analysis of attack patterns based on a review of the reported data breaches. Unlike other risk analysis reports drawing on insights from surveys of business executives or cyber risk professionals and experts from vendors who claim to have a crystal ball of the future, the DBIR tracks the year-on-year trend in historical cyber attacks.

**InfoSec Golf course**

DBIR used the analogy of a golfer navigating a golf course to explain how an adversary launches their attacks. The course creator builds sand traps and water hazards along the way to make life difficult. Additional steps, such as the length of grass in the rough and even the pin placement on the green can raise the stroke average for a given hole. These defences and mitigations are put in place to deter, detect, and defend. And just like on the golf course, the attackers reach into their bag, pull out their iron, in the form of a threat action, and do everything they can to land on the fairway. But this is where the similarity ends. The report observed that:

*"The first thing to know is that unlike a golfer who graciously paces all the way back to the tees to take his or her first shot, your attackers won’t be anywhere near as courteous. In Figure 29 we see that attack paths are much more likely to be short than long. And why not, if you’re not following the rules (and which attackers do?) why hit from the tees unless you absolutely have to? Just place your ball right there on the green and tap it in for a birdie or a double eagle, as the case may be."*

*(DBIR 2019)*

This is an unfair advantage when an attacker does not need to play by the rules. Figure 2 shows the number of attacks steps in the data breaches investigated in the DBIR 2019 report.



Figure 2: Number of steps per incident (n=1,285) Short attack paths are much more common than long attack paths. Source: DBIR 2019 report.

The composition of these steps, [the attack chains](https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html), were extracted and plotted in the form of colour-coded trails shown in figure 3. It displays the number of events and threat actions in the attack chains, by the last attribute affected.



Figure 3: Attack chain by final attribute compromised (n=941) Source: DBIR 2019 report

**Know your enemy**

Identifying the threat communities and threat actors are foundational steps in the FAIR scenario development phase. It is to inform the analysis on:

1. Who might launch the attack - cybercriminals, national-states, insiders?
2. The motivation for the attack - financial gain, espionage, innocent mistakes?

Table 1 is a sample analysis of these FAIR factors from the [FAIR Book](https://www.fairinstitute.org/fair-book):



Table 1: Quantified threat factors for the risk associated with the reduction in authentication strength for external website X. Source: FAIR Book

Figure 4 displays a high-level summary from the DBIR 2019 report on the identity of the threat actors and their motives. It shows a worrying trend of the rise in state-sponsored espionage which is difficult to defend give their massive available resources and sophisticated attack methods.



Figure 4: Summary of threat actors and motives in DBIR 2019. Source: DBIR 2019 report

The approach to use fact-based analysis to profile organisation risk underpinned [Wade Baker](https://www.linkedin.com/in/drwadebaker/)'s PhD dissertation "[Toward a Decision Support System for Measuring and Managing Cybersecurity Risk in Supply Chains](https://vtechworks.lib.vt.edu/bitstream/handle/10919/85128/Baker_WH_D_2017.pdf)". Table 2 is the risk profile of the organisations modelled in his research based on this approach. It shows the distribution of breach types against five industry types based on an in-depth investigation of nearly 1000 real-world data breaches occurring over a ten-year period.



Table 2 - Summary of breach types by industry. Source: Wade Baker PhD dissertation

Wade created and led Verizon's annual Data Breach Investigations Report effort while he was the Managing Director and CTO of Verizon Enterprise Solutions. Chapter 5 in Wade's PhD dissertation explained the rationale and development of the A4 data incident recording model (Actors, Actions, Assets and Attributes) expressed in the [A4 Grid model](http://veriscommunity.net/a4grid.html) format underpinning the [VERIS schema](http://veriscommunity.net/schema-docs.html).

**VERIS - a community effort**

[VERIS](http://veriscommunity.net/) is the vocabulary for event recording and incident sharing created by the DBIR team which underpins the analysis and publication of DBIR. The [VERIS community database](http://veriscommunity.net/vcdb.html) contains 8000+ incidents and is increasing daily thanks to an effort by the Verizon Security Research team members such as [Gabriel Bassett](https://www.linkedin.com/in/gabriel-bassett/) and other volunteers:



It is a far cry from the DBIR 2019 corpus covering 41,686 security incidents, of which 2,013 were confirmed data breaches. But it is a very useful resource to learn the VERIS schema and understand the analysis methodology behind DBIR. The [verisr toolchain](https://github.com/vz-risk/verisr), maintained by Gabriel is designed specifically to perform R analysis against the VERIS schema.

To put the DBIR 2019 report in the Australian context, Gabriel has kindly extracted [VERIS attributes related to confidentiality, integrity and availability](http://veriscommunity.net/enums.html#section-attributes) for Australian victim organisations. The results are summarised in figure 5:

1. 1905 incidents attributed to Australian victim organisations
2. Credentials and payment records were the prime attack targets
3. Malware and phishing attacks were most common
4. Ransomware was the most common cause of loss of availability



Figure 5: DBIR 2019 data set for Australian victim organisations. Source: DBIR 2019 data set

The best way to understand the DBIR analysis is to contribute to the VERIS community database by encoding data breach incidents using the [VERIS webapp](http://veriscommunity.net/veris_webapp_min.html#/). VERIS schema definition for attributes (<http://veriscommunity.net/enums.html#section-attributes>). Gabrial is running weekly VCDB coding sessions on the VERIS webapp tool via his [twitch TV channel](https://www.twitch.tv/gabe_the_engineer) and republishes the lessons through his [YouTube channel](https://www.youtube.com/channel/UCTGViRfVZwozbJtLxR05SKQ). It is a community effort!

In summary, the DBIR is a good source of information to model an organisation cyber risk profile when developing a scenario for FAIR analysis. It identifies the profile of the attackers and their motives targeting an industry sector. Practising risk analysis using the VERIS community (VCDB) database deepens this understanding.

**About the author**

[Denny Wan](https://www.linkedin.com/in/wandenny/) is a cyber security expert with over 20 years experience in the Australian IT security sector. He is the principal consultant of Security Express and the chair of the [Sydney Chapter of the FAIR Institute](https://link.fairinstitute.org/group/19-sydney-chapter) with deep expertise in Cyber Risk Economics. FAIR is an effective approach for prioritising cyber security investments and explaining its business values. He is a certified PCI QSA and CISSP. He is a postgraduate researcher at [the Optus Macquarie University Cyber Security Hub](https://www.mq.edu.au/about/about-the-university/offices-and-units/optus-macquarie-university-cyber-security-hub) researching into cyber risk management in the supply chains. This research is a useful tool for managing 3rd party supplier risks under compliance frameworks such as APRA CPS 234.

**About the reviewers**

[Gabriel Bassett](https://www.linkedin.com/in/gabriel-bassett/) is a senior information security data scientist on the Verizon Security Research team at Verizon Enterprise Solutions specializing in data science and graph theory applications to cyber security. He is the lead data scientist and a contributing author of the Verizon Data Breach Investigations Report. He supports several information security data science conferences and has previously held cyber security risk management, testing, intelligence, architect, and program management positions at the Missile Defense Agency and Hospital Corporation of America.

He is the maintainer of the [verisr toolchain](https://github.com/vz-risk/verisr) designed for the analysis of the VERIS Community Database. His YouTube video "[VCDB Data Analysis](https://www.youtube.com/watch?v=WuYPFpNp26s)" provides an excellent tutorial on the verisr toolchain.

[Wade Baker](https://www.linkedin.com/in/drwadebaker/) is a professor in Virginia Tech's College of Business, Co-Founder of the Cyentia Institute, and Advisory Board member for the RSA Conference and FAIR Institute. He had several prior roles all of which tie back in some way to his ongoing quest to improve cybersecurity knowledge, practice, and products through data-driven research. He is probably best known for creating and leading Verizon's annual Data Breach Investigations Report series – widely regarded in the industry for understanding threat trends and prioritizing defences.