The aftermath…

In September '22, Optus suffered its data breach and a few weeks later in October, Medibank announced that it had detected 'unusual activity consistent with the precursors to a ransomware event'. That's well-known history, but we just learned what actually happened.

On the 19th of this month, both barrels of the shotgun were fired when the Office of the Australian Information Commissioner (OAIC), and the Australian Communications and Media Authority (ACMA), both released separate filings with the Federal Court on the Medibank and Optus breaches, respectively.

Probably the most significant 'take away' (and good news!) from these filings is that protecting your technology and information assets from criminals does not have to be rocket science!

Establishing the fundamentals and assessing whether they are working as intended, will likely save your organisation from a similar situation (and if you need any help defining or assessing those, just drop us a note here).

The OAIC's 'concise statement' for Medibank, provides a good timeline of events of what happened. Debatably, a key failure was the lack of "Multi-Factor Authentication (MFA)" on a third-party 'privileged' account. There were other failures like not responding to alerts and warning signals when they were triggered.

But what was subtle, yet very important is the OAIC position that it was a "failure to implement or properly configure information security controls of *a basic or baseline nature* (emphasis added) or standard for an organisation of Medibank's size and in light of the volume and sensitivity of the personal information it held". In other words, the lack of MFA is now equated to a lack of a basic security measure. The writing is on the wall: password only authentication has got to go.

Finally, if you don't have enough examples – lack of MFA is noted as one of the key reasons why 'as many as 165 customers' of cloud storage provider Snowflake have caused breach headaches for organisations like Ticketmaster, Santander, and just recently Nieman Marcus.

What else? Review your 'Active Directory' for excessive or dormant privileged access – we do that a lot and you would be surprised just how bad it usually is. Also, conduct a 'red team' exercise to see if your Security Operations team (or Vendor) picks up on alerts or notifications. We might have done a similar thing for a similar organisation exactly eleven years ago with similar findings… so don't just test if it's working, but implement improvements when flaws are exposed – it's the follow through that's important!

The ACMA filing on Optus is similar in its ability to apply some sound 'lessons learned' for the benefit of the industry. This breach apparently is related to a 'coding-error'. That's understandable – we do LOTS of technical testing and we commonly see these types of errors – coding in a secure manner is tough at the best of times. What is NOT understandable is that the error was present for FOUR (4) years before the breach! What is also not understandable is that the error was found in one of two entry points (API's), but despite both being impacted by the same vulnerability, only one was fixed. If you are not assessing all your internet-facing systems (and API's) for flaws, errors or vulnerabilities, you can be guaranteed that *someone* is (aka the 'bad guys'). It's better you test them before they do!

And don't forget that you can't just aim a tool at a system and the answer pops out. Manual testing (coupled with automated) is highly valuable and why we do it with a team of experienced professionals, who do it all the time, and have done it for a very long time!

More "Real" Statistics

Last quarter Victoria Police told us they saw 11,000 cybercrime incidents related to the Medibank breach. This quarter we got more data. A register of stolen credentials created by the Federal Attorney General's Department (AGD) has apparently blocked over 300,000 attempts of identify fraud using the stolen identity details. That's a LOT of people who, fortunately, do not have to deal with identify theft, so kudos to the AGD! Breaches like these severely impact people's lives, so protecting against one isn't just 'good corporate behaviour,' but good for all of us!

Unprecedented, one-of-a-kind Google blunder?

As sceptical, old-school risk and cyber consultants when we hear words like 'unprecedented' used in the context of technology, you've got to expect a sharp, emotional response like "BULL$HI7!!"…

More serious KUDO's to UniSuper this quarter for dodging a lethal bullet which would have easily dwarfed the Optus, Medibank and Latitude breaches combined, in terms of exposure and impact.

Instead, it was quietly noted that UniSuper successfully recovered from an "'isolated, one-of-a-kind occurrence' never before occurred with any of Google Cloud's clients globally". This is significant because when we surveyed thirty 30 leaders in the technology/security/cloud space for our Cloud-focused Thought Leadership paper, and well over half (61%) did not know if DR plans had ever been tested and over half (56%) did not have DR plans in place if they lost the organisation's availability to the cloud resources. In fact, one participant was annoyed at the implication that they might need to do, what was essentially what they are paying for: "it's their job to ensure the data is protected and that's what we're paying them for" was the quote. Thankfully UniSuper didn't have that attitude and deserves a pat on the back for it!

The message should be clear: the cloud is NOT safe for your sensitive data – if you have data in the cloud that, if lost, would be catastrophic, then remember the 3-2-1 principle (or better) and TEST that it can be recovered. Many don't test and simply trust that it will work! Also aptly noted was that "service restoration wasn't just about restoring backups but also processing all the requests and payments that still needed to happen during the two weeks of downtime".

Why security matters.

An incident at e-prescription services 'MediSecure' caused ripples across the medical industry when it was not clear whether prescriptions in the Electronic Prescription Delivery Services were valid and could continue to dispense medications. But soon after being called out for taking an unacceptably long time to confirm how much data was compromised, they entered voluntary administration. A cyber incident will very likely happen to you – be prepared: have a plan and EXERCISE that plan to test how well you could respond to one. Hopefully then, it will not be an existential event!

———

Thank you for investing the time to catch up with us this quarter! If you're not already, please 'follow us' on LinkedIn and/or X (Twitter), and feel free to send this to others (or have them subscribe here).

Kind regards,

TrustedImpact
PROTECTING DIGITAL

we're **independent** consultants – it's about **your** business and **your** success
with a **singular focus** – cyber security is all we do
leveraging **experienced** professionals – credentials, not checklists