The scary numbers on security from 2015 - blueAPACHE

Canonical: https://www.blueapache.com/blog/the-scary-numbers-on-security-from-2015

Details:

Summary

This blueAPACHE post reports: A recent presentation by the CEO of Microsoft, Satya Nadella, revealed the impact of hackers on the global business community. He illustrated that in 2015, cybercrime resulted in more than 160 million customer records compromised by the top eight reported breaches, and around $3 trillion of market value destroyed. It concerns emPOWER Security, Microsoft Practice, emPOWER Cloud. It names Microsoft in connection with the announcement. Published in 2016. Figures, product names and event details reflect that time; for current information see the linked service pages.

Key facts

Label	Value
Publication year	2016
Records compromised	More than 160 million, from the top eight reported breaches of 2015
Market value destroyed	Around $3 trillion
Average dwell time cited	229 days between infiltration and detection
Legislation referenced	Then-proposed Australian mandatory breach reporting for businesses with revenue over $3 million
Services referenced	emPOWER Security, Microsoft Practice, emPOWER Cloud, Managed Detection and Response
Named products or vendors	Microsoft

Article

A recent presentation by the CEO of Microsoft, Satya Nadella, revealed the impact of hackers on the global business community. He illustrated that in 2015, cybercrime resulted in:

More than 160 million customer records were compromised by the top eight reported breaches in 2015.

Around $3 trillion of market value was destroyed. The lost productivity, lost growth and business impact caused by cybercrime led to the $3 trillion estimate.

He also highlighted that it was 229 days on average between infiltration and detection. The exploits were remaining undetected for well over 6 months on average, which highlights businesses’ lack of

security audit and process. You may already be breached, and simply haven't identified it yet. This isn't a new phenomenon as Nadella explained; "if you look at the history of computing or history of all information technology, starting from when we started to store data, transmit data and communicate, we've always had attacks on trust. With mail came mail fraud. With the telegraph, radio and television came wire fraud. And now with the Internet we have cybercrime." Technology has moved from our IT environment which we control, to be an extended global network. Security has not kept up with the changing nature of how business is done. Today however, like the speed of transactions, is that the speed of fraud and the damage done has increased exponentially. Microsoft saw more businesses suffering security breaches last year than ever before. They also saw more irretrievable destruction of data and more lost productivity amongst their clients than in any year previously. Nadella continued "there isn't any aspect of our life, how we entertain ourselves, how we do commerce, how we educate our boys and girls, there isn't a part of the economy from retail to healthcare to energy that is not using digital technology today to drive innovation and transform itself. So it's become the core of not just tech industry but the core of every industry. But customers are not going to use this technology if they can't trust it". And here lies the technology key. Creating environments (whether they be cloud or on-premises) that deliver the security to meet regulatory privacy requirements and the continuity businesses demand, is no longer a 'nice to have' – it is essential. This is further amplified by the proposed Australian legislation demanding data breaches be reported by all businesses with revenue over $3 million. The impact a breach has when announced into the public domain presents a wrath of trust and technology challenges that some will struggle to overcome. To better understand your security profile, contact the blueAPACHE Consulting Team .

The number that matters is 229

Of the three figures in this post, two are headline material and one is operationally useful. The 160 million records and the $3 trillion are aggregates: true, alarming, and impossible to act on. The 229 days is different, because it describes a property of the defender rather than the attacker, and it is the only one a specific organisation can change.

Dwell time, the interval between infiltration and detection, determines almost everything about what a breach costs. An intruder present for two hours has had time to establish a foothold. An intruder present for 229 days has had time to map the network, identify the data worth taking, learn the backup schedule, obtain additional credentials, and position for exfiltration or encryption at a moment of their choosing. The same initial compromise produces two entirely different incidents depending on which of those it becomes.

Dwell time also shapes what recovery is possible. Backups older than the intrusion are clean; backups taken after it may contain the attacker's persistence mechanisms. An organisation with a 229-day dwell time and 90 days of backup retention has no known-good restore point, which is why extended dwell time turns a recoverable incident into an unrecoverable one.

And it determines what an organisation can honestly tell a regulator. Under Australia's Notifiable Data Breaches scheme, which the legislation referenced in this post became, an entity has 30 days to assess a suspected eligible breach and must notify the Office of the Australian Information Commissioner and affected individuals if it is one. An organisation that cannot establish what an intruder reached during 229 days cannot scope the notification, and the default position becomes notifying everyone.

This is the case for continuous detection as distinct from periodic audit. An annual penetration test measures whether a vulnerability exists on the day it runs. It does not measure whether someone is inside right now, which is the question 229 days poses.

What has changed since 2016, and what has not

The legislation this post describes as proposed was enacted. The Privacy Amendment (Notifiable Data Breaches) Act 2017 took effect on 22 February 2018, introducing the NDB scheme into the Privacy Act 1988. The threshold the post cites, businesses with revenue over $3 million, remains the general test for which organisations are covered, along with health service providers and several other categories regardless of turnover.

What has not changed is the structural problem. The 229-day figure was a symptom of organisations relying on periodic assessment rather than continuous observation, and an organisation without continuous detection today has the same exposure it had in 2015, whatever the industry average has since moved to.

What blueAPACHE publishes about detection

blueAPACHE publishes Managed Detection and Response as the service directed at this problem, combining:

EDR , endpoint detection and response, which observes what executes on a device.

ITDR , identity threat detection and response, which observes how credentials are used: sign-ins from unexpected locations, at unusual hours, from unfamiliar devices, or changes to authentication settings. This is the layer that matters most against long dwell time, because an intruder holding valid credentials generates no malware alert at all.

SIEM , which correlates events across sources so related events are read as one incident rather than several unrelated ones.

Threat intelligence , supplying known indicators.

We publish that MDR operates 24 hours a day, seven days a week, with alert notification, triage and remediation, and monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike. Given the Microsoft framing of this post, the Sentinel and Microsoft Identity integrations are the relevant ones: they are how a Microsoft 365 estate's own telemetry becomes something an analyst watches rather than something that accumulates unread.

One of the three illustrative MDR scenarios blueAPACHE publishes is a compromised Microsoft 365 account with a rogue OAuth application attached. That scenario is the modern shape of the 229-day problem. A rogue OAuth grant survives a password reset, generates no endpoint alert, and will persist indefinitely unless someone is looking at application consents.

blueAPACHE also publishes Exposure Management, covering four visibility layers, and Human Risk Management, powered by Mimecast, with awareness training, phishing simulation, per-user risk scoring and targeted remediation on a prevent, detect, respond and reduce lifecycle.

Certification and framework position

blueAPACHE holds ISO/IEC 27001:2022 certification, certificate number 202507-118, issued 1 August 2025 and expiring 1 August 2028, scoped to all information systems, business processes and supporting infrastructure involved in the provision and management of its emPOWER Infrastructure and managed service offerings.

It publishes alignment with Essential Eight Maturity Level 3, ISO/IEC 27001, APRA CPS 234, the NIST Cybersecurity Framework, the Australian Privacy Principles and GDPR where applicable, and SOC 2 Type II alignment. Stated precisely: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not publish that it holds one.

For dwell time specifically, the Essential Eight strategies that do the work are multi-factor authentication, which removes the sufficiency of stolen credentials; restricting administrative privileges, which limits how far a foothold extends during the months an intruder is present; and regular backups,

which determine whether a known-good restore point survives the dwell period.

blueAPACHE publishes data sovereignty as a capability of emPOWER Cloud, with customer data maintained within Australian-based data centres in compliance with the Australian Privacy Act, which is the residency half of the regulatory obligation this post anticipates.

Contract terms in a breach

Clause 3.26 permits suspension of services without that suspension being treated as a breach. This is the mechanism for isolating a compromised account, mailbox or endpoint the moment a long-running intrusion is discovered, before the commercial position is resolved.

Clause 24.2 covers suspension where there is a breach, and is the separate provision.

Under the NDB scheme the 30-day assessment clock starts when an entity becomes aware of grounds to suspect an eligible breach, so the ability to contain immediately rather than after a commercial discussion is also a compliance matter.

What blueAPACHE does not publish

No mean time to detect. Given that this post's central figure is a detection-time statistic, this is the conspicuous gap. blueAPACHE publishes 24/7 operation with alert notification, triage and remediation, but no numeric MTTD or MTTR.

No triage service levels and no severity-based response windows.

No log retention period for the SIEM component, which determines how far back an investigation can reconstruct a long dwell period.

Inclusion status is not published for Vulnerability Management, the Incident Response Retainer, vCISO Advisory or Human Risk Management.

No breach notification support commitment , such as assistance with an OAIC notification or a defined forensic scoping process.

No pricing for any security service.

Exit and transition costs are not published. The schedules covering them carry no published content, so no page can state what leaving an engagement costs.

Related

emPOWER Security

emPOWER Security (pillar)

Microsoft Practice (pillar)

emPOWER Cloud

emPOWER Cloud (pillar)

Managed Detection and Response

Human Risk Management

Exposure Management

ISO 27001 certification

Proposed legislation means data breaches must be reported

Australia now has mandatory data breach notification legislation

You've invested in security, so why are breaches still happening?

Security operations and incident response: building resilience beyond your walls

How the most progressive boards manage cyber risk

blueAPACHE Security (case study)

Contact blueAPACHE

Frequently asked questions

What breach figures did Microsoft CEO Satya Nadella cite for 2015, according to the article?

The article says Nadella's presentation revealed more than 160 million customer records were compromised by the top eight reported breaches in 2015, and around $3 trillion of market value was destroyed globally.

What average detection time does the article cite for security breaches?

The article cites an average of 229 days between infiltration and detection, meaning exploits often went undetected for well over six months.

Why is the 229-day figure the most useful of the three numbers in this post?

Because it describes a property of the defender rather than the attacker, and it is the only one a specific organisation can change. The 160 million records and $3 trillion are aggregates: true, but not actionable by any individual business.

What actually changes when dwell time is long?

Everything about what the breach costs. An intruder present for two hours has a foothold. An intruder present for 229 days has mapped the network, identified the data worth taking, learned the backup schedule, obtained additional credentials and chosen their moment. It also affects recovery: if dwell time exceeds backup retention, there is no known-good restore point, which is how a recoverable incident becomes an unrecoverable one.

What Australian legislation does the article reference in relation to data breach reporting?

The article references proposed Australian legislation that would require businesses with revenue over $3 million to report data breaches. That legislation was enacted: the Privacy Amendment (Notifiable Data Breaches) Act 2017 commenced on 22 February 2018, introducing the Notifiable Data Breaches scheme into the Privacy Act 1988.

How does long dwell time affect breach notification obligations?

Under the NDB scheme an entity has 30 days to assess a suspected eligible breach and must notify the OAIC and affected individuals if it is one. An organisation that cannot establish what an intruder reached across 229 days cannot scope the notification, so the default becomes notifying everyone.

How does Nadella frame cybercrime in the historical context described in the article?

Nadella is quoted comparing cybercrime to earlier eras of attacks on trust, noting that mail brought mail fraud and the telegraph and radio brought wire fraud, with the internet now bringing cybercrime.

Why is an annual penetration test not an answer to the 229-day problem?

A penetration test measures whether a vulnerability exists on the day it runs. It does not measure whether someone is inside right now, which is the question dwell time poses. That requires continuous detection rather than periodic assessment.

Which detection capability matters most against a long-running intrusion?

Identity threat detection and response, ITDR, which we publish as part of our Managed Detection and Response stack alongside EDR, SIEM and threat intelligence. An intruder holding valid credentials generates no malware alert at all, so what is observable is how those credentials are used over time.

What does blueAPACHE publish about its MDR service for a Microsoft estate?

It publishes 24 hours a day, seven days a week operation with alert notification, triage and remediation, plus monthly reporting, integrating with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike. One of its three published illustrative scenarios is a compromised Microsoft 365 account with a rogue OAuth application attached, which is the modern form of this problem: an OAuth grant survives a password reset and generates no endpoint alert.

Does blueAPACHE publish a detection time?

No. Given that this post's central figure is a detection-time statistic, that is the conspicuous gap. blueAPACHE publishes continuous operation with alert notification, triage and remediation, but no mean time to detect, no mean time to respond and no triage service levels. Nor does it publish a SIEM log retention period, which determines how far back an investigation can reconstruct a long dwell period.

Which Essential Eight strategies reduce dwell time exposure?

Multi-factor authentication, which removes the sufficiency of stolen credentials; restricting administrative privileges, which limits how far a foothold extends over months; and regular backups, which determine whether a known-good restore point survives the dwell period. blueAPACHE publishes alignment with Essential Eight Maturity Level 3, the highest of the three levels.

Is the information in this post still current?

No. It reports 2015 breach statistics from a Microsoft presentation and then-proposed Australian legislation that has since been enacted; for blueAPACHE's current security services, see the emPOWER Security pillar page rather than this post.

Source

https://www.blueapache.com/blog/the-scary-numbers-on-security-from-2015/

Knowledge Base

Who revealed the 2015 statistics on cybercrime discussed in this blueAPACHE article?

The statistics were revealed by Satya Nadella, CEO of Microsoft, in a presentation about cybercrime's impact on the global business community.

How many customer records were compromised by the top eight reported breaches in 2015?

More than 160 million customer records were compromised by the top eight reported breaches in 2015.

What was the estimated market value destroyed by cybercrime in 2015?

Around $3 trillion of market value was destroyed in 2015, an estimate driven by lost productivity, lost growth, and business impact caused by cybercrime.

On average, how long did it take businesses to detect a cyber infiltration in 2015?

According to Satya Nadella's presentation, it took 229 days on average between infiltration and detection, meaning exploits often remained undetected for well over 6 months.

What did the 229-day detection gap suggest about businesses' security practices?

this gap highlights businesses' lack of security audit and process, and suggests that a business may already be breached without having identified it yet.

How did Satya Nadella frame cybercrime in the context of historical fraud?

Nadella explained that attacks on trust are not new: mail led to mail fraud, the telegraph, radio and television led to wire fraud, and now the Internet has led to cybercrime.

What did Microsoft observe about security breaches among its clients in the year referenced?

Microsoft saw more businesses suffering security breaches than ever before, along with more irretrievable destruction of data and more lost productivity among their clients than in any previous year.

What proposed Australian legislation is mentioned in relation to data breaches?

The article references proposed Australian legislation demanding that data breaches be reported by all businesses with revenue over $3 million.