NEW AUSTRALIA DATA BREACH RULES RAISE THE STAKES FOR MAINFRAME SECURITY

The cost of weak mainframe security just got a lot steeper. Following a series of high-profile, massive data breaches in Australia, the nation's government has just passed new legislation increasing maximum penalties for allowing such incidents more than twentyfold—to $50 million or more. Australian businesses are on notice: effective mainframe threat protection, detection, and response is now a top priority. As it should have been all along.

While numerous large Australian companies have suffered major data breaches in recent weeks, including Energy Australia, Telstra, G4S, Costa Group, MyDeal, and Dialog, two especially large incidents drew intense focus from both customers and lawmakers.

In September 2022, Australian telecommunications giant Optus disclosed a breach of the personal data of ten million of its customers—or roughly 40 percent of the entire population of Australia. The stolen data included not only names, addresses, phone numbers, and email addresses, but also especially sensitive information such as birthdates, passport numbers, and driver's license numbers.

The $1 million ransom being demanded by hackers is only the beginning of the company's problems, as possible class action lawsuits loom. As one local attorney noted, "This is potentially the most serious privacy breach in Australian history, both in terms of the number of affected people and the nature of the information disclosed."

Just weeks later, health insurer Medibank Private suffered a breach that compromised the medical information of 9.7 million people—some of which was subsequently released on the dark web. In

addition to customers' names, birth dates, and passport numbers, the hackers revealed information on medical claims filed by these individuals, including sensitive procedures such as miscarriages and terminated pregnancies.

As private personal data continued to flow through porous enterprise defenses and into the hands of hackers, Australian legislators decided that they'd seen enough.

The soaring cost of a mainframe data breach

The recently passed Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 represents more than a merely incremental increase in fines. Since 1988, companies allowing serious or repeated privacy breaches have faced a penalty of $2.2 million. Starting now, they can be forced to pay whichever is greater of:

- $50 million
- Three times the value of any benefit obtained through the misuse of information
- Thirty percent of the company's adjusted revenue in the relevant period

Attorney General of Australia Mark Dreyfus justified the increased penalties given the role that lax mainframe security played in allowing such breaches to occur, saying, "Unfortunately, significant privacy breaches in recent weeks have shown existing safeguards are inadequate. It's not enough for a penalty for a major data breach to be seen as the cost of doing business."

And regulatory fines are only part of the cost of a mainframe data breach. According to IBM, additional post-attack expenses typically encompass investigations; crisis management; communications with customers, regulators, and lawyers; business costs including downtime, lost customers, and reputational damage; and legal expenses.

How BMC helps customers avoid data breaches—and the resulting penalties

Most mainframe organizations are already well aware of the urgency of strengthening data protection. In the latest BMC Mainframe Survey, 67 percent of respondents cited security and compliance as their top priority, a six-point increase over last year. Much work remains to be done; 80 percent of respondents reported that a security audit had identified vulnerable user accounts, while 34 percent found that their mainframe had been accessed in an unauthorized manner.

BMC helps customers strengthen mainframe data protection with solutions including BMC AMI Security, which leverages artificial intelligence and automation to continuously detect and respond to threats on the mainframe. Automated protection, detection, and response capabilities scan databases for suspicious activity in real time and halt malicious actions even before systems are compromised. To accelerate incident response, BMC AMI Security correlates data across multiple systems and translates it into common security terms for clear, actionable intelligence. Integration with leading security information and event management (SIEM) tools and BMC Helix enables real-time visibility so security and IT operations (ITOps) teams can see all actions occurring on the mainframe with a timeline of actions to quickly investigate security incidents.

Even before a threat has been identified, BMC AMI Security performs continuous policy scanning to uncover configuration vulnerabilities so mainframe teams can proactively close security gaps.

Granular reporting provides detailed insight into threat events, suspicious activity, and regulatory compliance risks, while real-time alert and audit trails help improve adherence to standards including the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), and General Data Protection Regulation (GDPR).

The newly passed Australian privacy law is only the latest move by legislators and regulators worldwide to increase the cost of lax data protection—and it won't be the last. As mainframe teams in Australia and elsewhere seek to strengthen the security of this business-critical platform, they'll need to leverage the full power of automation, artificial intelligence, and integration to stay one step ahead of hackers. BMC can help. To learn more, explore BMC AMI Security.