Howzat! Welcome to the Ashes Cyberline series

Talking point
Ben Flatgard

As Starc and Hazlewood were knocking over the English resistance in Perth, Australian hackers have been deploying a “Cyberline” approach of their own. According to new charges filed in Federal Court this morning, a computer associated with Cricket Australia was used to illegally access the England Cricket Board’s private servers. The Australian camp has denied accusations that it stole player injury reports as well as the batting, bowling and fielding strategies England deployed in the first Tests. There is no indication this information would be used to inform an alleged spot-fixing scheme.

The revelation comes on the heels of the MCG announcing a computer compromise in the system — called DRS — that enables review of umpire decisions at the ground. Preliminary reporting of the incident suggests a so-called “ransomware” attack, which holds a computer hostage until payment is made. Both teams have agreed to scrap the review system in Melbourne over fears of reliability and integrity.

Fear not — the tiny urn is still coming home, but it will not be filled with subpoenas. While England has been left looking for scapegoats, “Cyberline” tactics cannot be blamed. Hawk-Eye and DRS have caused some controversy, but not (yet) due to a ransomware attack. The quality of the play may be in question, but the integrity and spirit of cricket have not been compromised.

Thankfully cybercrime has not yet hit cricket, but the scenarios described above should look familiar to Australian businesses. Australia’s critical infrastructure — electrical grid providers, mine operators, banks and defence contractors — is being targeted. It may not be the theft of team batting strategies, but it is often the theft of sensitive business or customer information. The disruption of the DRS system in the example above is exemplary of the real peril businesses face from online extortion schemes. Just look at the Tasmanian chocolate factory that was shut down due to a ransomware attack this year.

Just like a good forward defence, solid fundamentals are still the best way to defend ourselves against cyber attack. The Australian government has put out an “essential eight” set of security practices that every business should look to adopt. These simple steps, such as utilising fingerprints for system login or updating software when it is made available, will protect companies from many of the most common attacks.

But even the best defence will occasionally fall to Jimmy Anderson’s reverse swing or Nathan Lyon’s sharp spin. Just blocking the ball back will only work for so long, eventually a sophisticated attack will find a way through.

To gain resiliency, companies need to understand and mitigate the cyber risks posed to their business. Developing such an understanding does not require technical expertise. It requires considering what business functions are crucial and what data cannot be lost. There are open-source frameworks, such as one created by NIST, to help with this process. Once you understand the risks your company faces, you can put in place technical cyber protections as you might add vendors to diversify a supply-chain or insurance products to protect a balance sheet. Resilience is efficient and sustainable. Efficient in that you know where your wicket is — you only deploy security solutions that protect your most critical datasets and applications. Sustainable in that you accept your defence will sometimes fail.

You might lose your opening partnership, but that doesn’t mean the whole innings needs to collapse. Critical data will be backed-up, key operational systems will have manual fall-backs, and you will be better prepared to communicate with customers and business partners during cyber incidents.

Partnership is crucial in cyber security and government-private sector teamwork is perhaps most important when it comes to sharing information about cyber-threats.

When one organisation is targeted, it can share the details about the attack. The Australian government is now setting up hubs for this information sharing — called Joint Cyber Security Centres — in each state capital. All businesses should look into how they might contribute.

The opportunity for co-operation extends beyond Australia’s shores. Last year, Australia was the first country to join the cyber information sharing network established within the US. Unlike on the cricket oval, Australia and Britain have a long history of co-operation in cyber security. Both countries are committed to an “open, free, and secure” internet. They have worked together to advance international norms that establish what is “just not cricket” when it comes to online behaviour.

Enforcing the rules may be more difficult than getting a batsman to walk in the age of instant replay. Attributing cyber attacks to responsible individuals is difficult. Enlisting the co-operation of third-party countries to bring criminal charges requires persistent diplomacy. But despite the challenges, there is a proven track record of success.

This month, Australia joined a multinational coalition to dismantle one of the world’s largest hacking networks and put its mastermind behind bars. Hitting a consistent line and length through law enforcement co-operation can generate pressure and send the wickets tumbling.

Ben Flatgard is the 2017 Alliance 21 Fellow at the United States Studies Centre at the University of Sydney. He is former director for cyber security policy on the US National Security Council under President Barack Obama.

Luckily, DRS hasn’t been hacked during the Ashes series. PHOTO: AAP