Financial services organisation

Client name: Financial services organisaton

Location: Australia and New Zealand

Industry: Financial services

DXC.technology

Challenge

- Protect and secure valuable data
- Comply with strict regulatory guidelines
- Proactively search for and destroy network weak points

Solution

- Conduct network penetration testing and black box testing
- Identify threats and report findings
- Consult on results and next steps

Results

- Regulatory compliance
- Enhanced cybersecurity awareness among C-suite
- Greater peace of mind

When the best form of defence is attack

Superannuation administrator maintains robust network security with DXC Technology's strategic cybersecurity services.

Attaining deep cybersecurity knowledge is essential in the ongoing war against hackers and other cyber criminals. Across the globe, enterprises must contend with ongoing cybersecurity threats. Organisations providing IT security must comply with minimum security baselines and government regulators have set common standards for specifying and evaluating security in IT products and systems.

CIOs need to continually monitor the evolving threat landscape and replace an 'if we get hacked' mindset with a 'when we get hacked' mindset.

The Head of Information Security at a leading superannuation administration organisation concurs with this. The organisation is a share registry and financial services provider in Australia and New Zealand, managing over 10 million superannuation and pension member records and more than 1,000 ASX securities records.

With such valuable data in its care, the company must comply with strict auditing and regulatory guidelines set by the Australian Prudential Regulation Authority and other international bodies. Compliance requires regular cybersecurity security assessment by an independent company.

Not content with just meeting its regulatory baseline, the company commissioned DXC to conduct extensive network penetration testing. This testing resulted in a deeper understanding of what the Head of Information Security calls the company's "low-hanging fruit" — internet-facing systems that may have been vulnerable to hacking attempts. "Most importantly, it shone a light on which initiatives were working well, and what we could improve," he says.

Keeping hackers at bay

DXC had conducted annual network penetration testing for a number of years on a subsidiary company of the organisation that provides administrative support to Australian superannuation funds.

"DXC came to my notice through its consistently good work with our subsidiary," explains the Head of Information Security.

An opportunity arose for DXC to conduct a larger penetration test for the organisation, after subsequent acquisitions resulted in the management of a larger share registry.

"This was the real test for DXC — their moment to prove themselves," says the Head of Information Security. "And they did. DXC performed well and met our timelines and criteria for testing and reporting, so we asked them to take on additional projects."

"In the past, the approach we took to testing our web portals and networks was based on a defined scope, typically for compliance purposes. The approach wasn't modular or all-encompassing, so it didn't truly reflect how or what black-hat hackers would target in real life."

"This was the real test for DXC — their moment to prove themselves. And they did. DXC performed well and met our timelines and criteria for testing and reporting, so we asked them to take on additional projects."

– Superannuation Administrator
Head of Information Security

DXC Cybersecurity consulting performs threat intelligence analysis

Information security strategy is traditionally based on generic best practice, compliance or standards, and is often developed in isolation to real-world threats faced by organisations.

The company's strategy followed this same path. The Head of Information Security knew the company's existing strategy provided a base level of defence, with some additional protective measures for known or perceived critical assets. However, he wanted to take the organisation's threat intelligence strategy to the next level by testing its entire online presence.

"In the past, the approach we took to testing our web portals and networks was based on a defined scope, typically for compliance purposes," says the Head of Information Security. "The approach wasn't modular or all-encompassing, so it didn't truly reflect how or what black-hat hackers would target in real life.

"We wanted to know what our vulnerabilities were upfront, rather than find out the hard way by being exposed and losing data."

The superannuation administrator commissioned DXC to perform a group-wide penetration test on its entire online presence, which comprises more than 200 websites and a wide IP address range. DXC used a black-box methodology — known as 'ethical' or 'white-hat' hacking — over the course of several weeks to probe and assess the organisation's network environment.

To ensure the black-box scenario is as close to real life as possible, DXC's white-hat experts are given little to no background information about the client or its networks.

The DXC team worked within a timeframe specified by the company, and in a way that didn't disrupt its normal business activity.

DXC followed up with detailed reporting and analysis of its findings, which helped the organisation establish greater awareness of its security posture. These findings also highlighted the importance of strong cybersecurity governance to other C-suite executives.

"It gave us peace of mind," says the Head of Information Security. "We gained a clearer understanding of where our weak points were and, if we were targeted, how hackers would expose vulnerabilities and access our network."

In future, the company plans to commission additional black-box testing to further strengthen its information security systems. According to the Head of Information Security, the important role proactive network penetration testing plays to the organisation can't be stressed enough.

"The internet and its associated networks are becoming more hostile every day," he says. "It's basically an arms race out there. To effectively manage data security risks, organisations must be proactive about their defence. DXC helps us do that."

DXC_CSC-306. March 2017