PROTECTING YOUR DATA:

The information security measures integrated into everything we do at Computershare

April 2024

There are many factors to consider when selecting a partner to manage components of your business – expert knowledge, service quality, technology, cost – but one of the most important is that partner's approach to information security.

At Computershare, a world leader of financial administration services, we take the security of your information as seriously as you do. With 40,000+ clients, representing millions of stakeholder records, we take every precaution to protect the data we are entrusted to hold. We manage 850 meetings each year in Continental Europe and 7,500 meetings globally, with meeting and shareholder data securely protected within our systems.

Information security framework

As a global service provider, Computershare's information and cyber security procedures adhere to regional requirements across the jurisdictions where our clients conduct business.

As such, our procedures are robust, continually invested in and tested, and overseen by a dedicated team of in-house information security experts.

Our global information and cyber security framework is aligned to ISO/IEC 27002:2013, an international set of guidelines established by the International Organisation for Standardisation on best practices for managing information security.

This framework, which covers all Computershare business units and geographic locations, including Europe, is in place to:

- Continuously perform assessments against cyber risk and threats, and protect highly sensitive client data from breaches, unauthorised access, malware infections, and Distributed Denial of Service (DDoS) attacks.
- Comply with regulatory requirements across the globe. The EU General Data Protection Regulation (GDPR), the most significant change in data protection law in the last 20 years, gives individuals more control and rights over their personal data. Computershare's systems are compliant with GDPR and have controls in place to safeguard the security of personal data and ensure it is processed in line with those requirements.

Our risk management policy and framework, aligned to ISO 31000 guidelines, monitors risk management measures consistently across all business units.

This framework supports Computershare's risk objectives by bringing a consistent approach to identifying, analysing, mitigating and reporting risk and control within acceptable tolerances.

Both our information and cyber security and risk management frameworks are reviewed by Computershare's business and technology groups and approved by our Board.

Information security infrastructure

Our IT network and supporting technologies (network gateways, switches, routers, firewalls, servers) are managed and controlled by Computershare's Technology Services group.

The technical security controls incorporate security architecture principles (i.e. defence-in-depth, least privilege, default deny and fail secure) and security hardening guidelines (i.e. utilise secure encryption protocols and disable insecure protocols/versions).

Our defence-in-depth methodology uses various technologies and deployment locations to mitigate the effects of a DDoS or SYN/FLOOD attack. We use multiple internet service providers to reduce the attack surface through various failover options, as well as other traffic routing and monitoring equipment for further protection.

We have robust monitoring and alerting protocols in place at the network, application, and server level to provide visibility in real time of our system performance. Incident response plans, including specific procedures for DDoS-type attacks are in place to enable detection, containment, eradication and recovery from any such attacks.

Information security programs

When it comes to maintaining information and cyber security, the scope is broad, and many scenarios must be accounted for to protect the confidentiality of client records and the privacy of shareholder information.

The programs we have in place to continually safeguard and survey our security landscape address the following:

- Data governance and classification
- Systems and network monitoring
- Asset inventory and device management
- Systems and application development and quality assurance
- Access controls and identity management
- Physical security and environmental controls
- Business continuity and disaster recovery planning
- Customer data privacy protection
- Systems operations and availability concerns
- Vendor and third-party service provider risk assessments
- Systems and network security management
- Incident response management

Information security 24 x 7 x 365

With the potential for cyberattacks always in play, Computershare is ever vigilant. We proactively monitor for newly emerging threats, trends and increasing regulatory demands.

Our centralised Security Operations Centre provides around the clock coverage that is always monitoring, analysing and responding to suspicious events. Computershare uses internal and external parties to actively monitor the internal and external threat environment and test the security stance of applications and their underlying infrastructure.

We also operate regular assurance controls to independently validate and track threats, and report to management that the required measures have been taken to address and control the potential technical issues discovered during testing.

Penetration testing, conducted by external firms, takes place on an annual basis for critical applications. We also commission several external audits to provide an independent assurance and attestation of our business and technology controls.

These external audits include System and Organisation Controls (SOC), International Standard on Assurance Engagements (ISAE) 3402, Statement on Standards for Attestation Engagements (SSAE) 18, Australian Standard on Assurance Engagements (ASAE) 3150, and ISO 27001:2013 that are applicable to specific business units and geographic locations.

Dedicated, experienced and qualified information security teams around the globe

27,000+ of our most privileged system accounts protected with our enterprise grade password management tool

'Advanced' Security Rating from Bitsight Technologies, the industry's preferred rating system

8,000+ hours spent by Computershare staff on mandatory information security e-learning

2,000+ client security engagement completed

3,500+ hours ethically hacking and technically assessing our own systems

Daily automated vulnerability scans against our perimeter networks and internal assets

24 x 7 Security Operations Centre with all year round global coverage

0.8+ million access entitlements certified

Millions invested in information security each year