Management Approach: Cybersecurity and Privacy

Cybersecurity attacks can disrupt our business operations, resulting in financial losses and reputational damage. To address this risk, Stantec has implemented world-class security systems, security policies, processes, and practices and invested in staff cybersecurity awareness training to help reduce the risk of network and system breaches.

Furthermore, we are committed to respecting and protecting the privacy of individuals and ensuring that all personal or sensitive data within our possession or under our control is handled with due care. As part of the global risk management (legal) function, our Privacy Officer oversees such programs.

Stantec protects our systems and the people who entrust us with personal information in various ways:

IT Service Management
Stantec is one of the few architectural and engineering firms to maintain an ISO 20000-1:2018-certified IT Service Management System (part of our Integrated Management System). This certification ensures service delivery processes (including security) meet the quality standards set by the British Standards Institute.

IT Security Management
Our IT security programs maintain data confidentiality, integrity, and availability (whether data is stored on our premises or in the cloud). Comprehensive security systems include web filtering, intrusion protection, multifactor authentication, cloud access monitoring, cloud-based email filtering, next-generation firewalls, and advanced endpoint protection, detection, and response. We have stringent requirements for external access to our systems and wireless network.

Stantec has platform-integrated IT fraud detection systems, and our programs are subject to regular audit. The director of Enterprise Risk Management leads an Integrity Management team and Fraud Risk Assessment Program. Any actual or potential security problems are reported to the chief information officer, Risk Management team, or Integrity Management team, as appropriate.

As well, Stantec is in the process of certifying against the ISO 27001 information security standard. which includes an Information Security Management System scoped to address personal, financial, and client information. As a core component and to address the increasing variety and sophistication of cyberattacks and threats, Stantec has crafted a new Information Security Policy. The purpose of this policy is to safeguard information belonging to, or entrusted to, Stantec and its stakeholders. This policy informs Stantec employees of the principles governing the holding, appropriate use, and disposal of Information.

Privacy Management
Stantec's privacy program complies with applicable laws, including the General Data Protection Regulation (European Union), Defense Federal Acquisition Regulation Supplement (United States), and Cyber Essentials Plus (United Kingdom).

The program limits the collection and use of data to only what is needed to operate our business (a more in-depth policy and practice is available internally to Stantec's systems for use by employees). In accordance with legislation, our programs ensure the accuracy, confidentiality, integrity, and security of information, and provide the right to request and correct data.

Stantec posts an external facing Privacy Notice as a public statement to people whose data we may collect, use, and process to explain what we collect, what we use it for, and how we protect it. Also included is key information about who to contact and what rights individuals have concerning their data. Our internal facing Privacy Policy outlines how all Stantec employees should act and behave when using or accessing the personal data we collect.

Stantec maintains a single centralized point of contact for raising privacy-related issues and concerns at privacy@stantec.com.

Incident Response
Stantec tracks cybersecurity and privacy incidents and has a robust incident response program in place should the necessity to invoke it arise. Underpinning our Security Incident Response program is a robust system that orchestrates incident response activities and provides multi-jurisdictional information about breach notification regulations.

If a potential cybersecurity breach were to be identified, the IT Incident Response program is immediately invoked to identify, investigate, contain, remediate, eradicate, and recover from the threat.

Training and Communication
Technology is not enough to fully shield us from cybersecurity attacks and privacy breaches. We also need our employees to identify—and stop or report—problems as soon as they see them.

Our comprehensive IT Security and Privacy Training gives employees the tools required to do this, and communication from management keeps employees informed about protecting assets and thwarting scams.

See Also
Management Approach: Integrated Management System