"Governance

Designated CISO, CIO, and Chief Privacy Officer in place.

Colgate conducts mandatory information security and privacy training for employees and contractors which covers social engineering, privacy/data handling compliance, security/threat awareness, and phishing campaigns. In addition, they conduct further role-based training. Click rate for phishing simulations is less than 15%.

Colgate's employees have been educated to report phishing emails via a button integrated into their corporate email system. Annual cybersecurity mandatory training ensures that employees understand how to report data security incidents to their IT Help Desk which is available 24/7. They also have specific Data Privacy training which is mandatory for all employees.

Incident Response infrastructure in place that includes plans, defined roles, training, communications, and management oversight.

SOC reports incidents to Audit Committee on a quarterly basis.

Privacy

A Chief Privacy Officer is in place. Colgate only holds employee PII totaling 31,692 individuals. B2B business. No customer records maintained.

All sensitive data that is held is encrypted. Data Loss Prevention tools in place. Data Privacy training is mandatory for all employees. Least privileged utilized to limit access to sensitive and critical data.

At our attachment point of excess $50m, Colgate is a very low privacy risk.

Network Security

100% of the enterprise is covered by vulnerability scans. They do not use Office 365 on the network (they are a Google Workplace shop). At least annual third party penetration tests on all externally facing systems. Tabletop exercises conducted including ransomware specific.

Last ransomware tabletop was performed in November 2020. Monthly risk assessments performed to determine if firewalls are blacking all unnecessary services. Monthly web application asset discovery scans performed.

Quarterly risk assessments performed for external server and internal server environments.

WAF in front of all externally facing applications, and it is in blocking mode. Colgate utilizes an external service to monitor its attack surface.

24/7/365 SOC (via MSSP). SIEM too log and intake. Colgate has SOC members in both the US and India, covering the EST and IST business day, Monday to Friday. Additionally, team members are on-call 24/7 with rotational on-call shifts. Multiple MSSPs provide 24/7 coverage for both monitoring and detection. RTO to triage and contain security incidents is between 30 minutes and 2 hours. They monitor the network traffic for anomalous and suspicious data transfers.

Endpoint Isolation and Containment technology is utilized.

IT and OT environments are segregated. For the manufacturing environment the equipment/software is segmented by firewall from the rest of the network. The network is segmented by geography so that traffic between offices in different locations is denied unless required to support a specific business requirement.

Colgate has one global data center, with a majority of remote locations directly connected to the global data center. Specific high risk geographies have been identified by the IT leadership team for segmentation. Segmentation also exists within the global data center, leveraging a segmentation firewall. Critical servers are segmented from users, printer, wireless, etc.

If they have any EOL software they either buy extended support or decommission the software.

Ransomware and Business Interruption

MFA is in place for all remote connection into the network for employees and vendors. Employees access to the corporate VPN requires both a managed device, username, password and MFA. All access to Google's Workspace quite requires both a managed device, username

and MFA. All contractors that access the network do so via corporate VPN that requires both username, password and MFA.

Colgate has a third party engaged to provide remediation services. They also have a cybersecurity incident response firm under contract to immediately respond to a ransomware incident as part of their IRP. Red team in place internally and they utilize a third party red team to test their defenses. They leverage Security Scorecard, Bitsight, and Cycognito to identify security vulnerabilities for systems exposed to the internet.

Users cannot run MS Office Macro enabled documents on their system. This is disabled by default on all business user machines.

EDR (Cybereason and Microsoft Defender to provide multiple layers of protection) is deployed on all endpoints and IT supported servers. All workstations have antivirus with heuristic capabilities. Colgate uses endpoint security tools with behavioral-detection and exploit mitigation capabilities. They have an internal group which monitors the output of endpoint security tolls and investigates any anomalies.

Strong email controls. Colgate utilizes multiple email protection solutions in order to provide a layered defense for email. One system protects messages at the gateway level, and second layer provided by Google's Workspace platform. They utilize Palo Alto Networks for web filtering globally as well as categorization of websites for blocking. Both email protection solutions leverage sandboxing for suspicious attachments. Email filtering solution used to block suspicious messages. All external emails are flagged as having originated from outside the organization. SPF and DMARC in place.

Employees do not have local admin rights. Colgate leverages Microsoft LAPS and CyberArk for PAM solution. All exceptions are reviewed by a governance and approval process by senior IT management. Admins have unique, privileged credentials. Privileged accounts require MFA. Passwords kept in a vault. Log of all privileged account use. Their system administration team utilizes a Jump Server for admin access to critical systems. Access to the jump server is controlled with MFA via Colgate's corporate IDP provider. Centrify is their PAM.

Patch management strategy, which includes critical patches, requires first applying the patch in their dev system. They then promote the patch to their test system and Quality Assurance. The final step occurs during regular scheduled production maintenance where production systems are patched. This strategy is followed for all patches that are managed by IT. Patches which require an exception to this process (e.g. zero-day) must be approved by IT leadership team.

All backups are encrypted both on-site and off-site. They test the integrity of backup-ups prior to restoration to ensure free from malware on a regular basis. Backups include offline backups stored onsite, offline backups stored offsite. They utilize multiple different backups technologies which are not dependent on Active Directory. These are both on-premise and fully disconnected off-premises, plus an additional real-time replication disaster recovery site exists outside of Colgate's managed infrastructure. The DR site is hosted and managed by IBM. They have a policy that utilizes full disk encryption via Bitlocker for all workstations globally.

BCP, DRP, and IRP in place and tested at least twice annually. RTOs for critical systems is 4-24 hours.

Vendor Management

MFA is in place for all remote connection into the network for vendors. All contractors that access the network do so via corporate VPN that requires both username, password and MFA. Most contractors must utilize Colgate managed laptops when critical system access is required. MFA is performed via SMS, Authenticator app or voice call leveraging Colgate's global investment in Okta for Identity and Access Management. Okta used for single sign on to all corporate applications.

In addition, Colgate utilize a third party service provider to conduct an extensive vendor review prior to utilizing their services. The level of detail is based on the risk assessment done by the business and security together. These reviews are reviewed on an annual basis and also when the scope of the vendor services changes. This information is all tracked in a central database and additionally reviewed by our internal corporate audit organization. Typically, Colgate contracts with vendors include indemnification by the vendor for claims arising from material breach of the contract (including breaches of the confidentiality, data security and data privacy terms), negligence and willful misconduct, intellectual property infringement, personal injury and damage to property

Media

Colgate has a formal review process whereby any media content is reviewed by a cross-functional team, including legal, to assess potential for infringement or other legal issues.

Manufacturing is well within EmergIn's risk appetite at the appropriate attachment point. Colgate is a very low privacy risk with only 31,000 employee records maintained. Pure ransom/BI risk. At our attachment point of xs $50m, I'm able to get comfort around this account given strong network security controls around EDR, intrusion detection and prevention, strong documented patching cadence, annual third party pen tests, red teaming,

regular tabletop exercises (including around ransomware), MFA for all remote access and for administrative and privileged access, strong backup procedures and RTOs, BCP, DRP, IRP (with ransomware playbook). I believe given the foregoing, we can gain comfort renewing this account on an excess basis as $5m po $20m xs $50m @ $134,070 (22% increase at renewal). This represents 85% ILF of underlying Starr terms "