ZoomInfo Security Overview

1. Introduction

ZoomInfo is a Vancouver, Washington-based software company providing subscription-based SaaS services to over 15,000 companies worldwide. For 20 years, ZoomInfo has assisted companies in achieving profitable growth. ZoomInfo assists its clients in identifying ideal prospects and decision-makers within their target market.

2. Our Commitment to Security

ZoomInfo is a security-first organziation committed to protecting our information from intentional or unintentional misuse. This includes customer, partner, vendor, and other third-party information.

In this spirit, ZoomInfo is proud to have implemented a robust Information Security Management System ("ISMS") that meets the strict guidelines of the ISO 27001 Standard. We have also earned AICPA's SOC2 attestation regarding the security, availability and confidentiality controls around our services. Our ISMS includes within it the Risk Management program formally based on the ISO 31000 Risk Management Framework.

Regulations and Laws

Compliance

Certifications

Due Diligence

Customers

ZoomInfo complements its security team's expertise with industry-best tools and third-party services. These services include assessments, controls reviews, technical reviews and testing. Tools are integrated into our process lifecycle and we employ various continuous control monitoring functions throughout our environment. In addition, we have additional supplementary security protections in place to deflect and thwart exploitation attempts.

As part of our security framework, we carefully review our service providers' security practices, requiring appropriate certifications which may include SOC 2 Type II, ISO 27001, PCI DSS, HIPAA, and CSA-STAR, and perform an analysis of control to ensure we manage third party risks to ZoomInfo.

3. Security Fundamentals

Our risk management and compliance framework provide the basis for our information security program. The core of the program is defined by our ISMS and serves to assess, manage, monitor, and minimize our information security risks. The program includes:

- ✓ Context of the Organization
- ✓ Leadership
- ✓ Planning
- ✓ Support
- ✓ Operation
- ✓ Performance evaluation
- ✓ Improvement

The ISMS provides the structure from within which we perform the various tasks required to maintain and refine the program. It consists of a set of policies and procedures that help ZoomInfo formally and systematically manage our sensitive information. These policies and procedures address the risks related to who has access to our information, the processes in which they handle that data, and the technology employed to manipulate it. It affects the way people work and how they behave. Proper employee conduct in handling sensitive information is reinforced by a dynamic information security awareness training regimen. Our awareness training function provides consistent instruction that not only influences the behavior of the individual, but also serves to influence the ZoomInfo corporate culture ensuring the progression to a single, more security-conscious global corporate entity.

4. Security Team

Our information security team is comprised of seasoned security veterans with experience managing all facets of information risk including compliance, risk management, Cyber Security Operations Center (CSCO), security engineering and offensive security. Members of our team hold certifications including Certified Information Systems Security Professional (CISSP), Certified Information Systems Management (CISM) and Certified Information Systems Auditor (CISA) and many have relevant military experience related to information security. All of our staff participate in continuing education and training throughout the year ensuring we are implementing ever-evolving best practices.

Our information security policy outlines the roles and responsibilities within the organization, and our security team works directly with specific members of senior management we call “security partners” to ensure that the various information security directives are executed as required in their respective departments. Our security partners help to establish, assess, and enhance business processes by ensuring the required information security risk management practices are suitably embedded within their respective processes.

Cyber Security Operations

- SOC Management
- Phishing
- Awareness
- Face to Face New Hire
- Playbooks

GRC

- Audit
- Compliance
- Certifications
- Vendor Risk
- Auditing
- FRP Responses

Offensive

- Pentesting
- Red team
- Vulnerability Management
- SAST
- DAST

Cloud Compliance

- S-SDLC
- Cloud Security Architecture
- Cloud Audit
- Cloud Security Configuration

Security Engineering

- Security Tools Management
- Security Tools Implementation
- Integration of events to SOC
- Supporting other teams

5. Risks and Opportunities

ZoomInfo's ISMS implementation allows for the appropriate integration of security processes and controls into the existing or newly created processes. This enables security to be part of a process and not an afterthought. Appropriate metrics are provided to executive leadership for effective management of risk and improvement of controls. ZoomInfo's risk management platform is anchored to the ISO 31000 Risk Management Standard, and continuous risk assessment activities are conducted in partnership and coordination with risk owners affiliated with the various ZoomInfo business units.

6. Our Staff and Internal Operations

All of our employees are carefully vetted and subjected to background checks or equivalent (based on country laws and practices) prior to hiring. Employees are scrutinized not only on previous experience, but also on how well they fit into the overall corporate culture.

Current employees are required to participate in continuous and dynamic awareness training that is designed to develop and maintain a security-focused culture. The training program seeks to empower our employees and consultants to make responsible, secure decisions and to protect our most valuable assets. We employ a variety of tools, techniques, and programs to embed security into our professional and personal lives.

All employees and contractors are required to successfully complete an annual, interactive security training program that includes an overview of key security topics, policies and responsibilities, and all new employees are required to complete this training shortly after their onboarding.

Specialized staff such as developers and security personnel undertake additional training specific to their roles. Additionally, all employees and relevant contractors are required to review and acknowledge our information security policies, including our Code of Conduct and Acceptable Usage Policy.

Consistent and repetitive interaction with our user base is an integral part of our security awareness initiative. The message that "security is part of everything we do" is driven home by numerous information streams. Regular security bulletins are disseminated across all spheres of the organization with tips and best practices, external security resources, emergency response information, security alerts, awareness information, security procedures, and contact information for associates and contractors to ask security-related questions or raise concerns.

Overall, the Security Training and Awareness program consists of various methods of delivery. Examples of tools employed: classroom-based training, Zoom meetings, updated infographics, posters and other visual aids, online training, videos, blogs and portal articles, newsletters, internal social media feeds, intranet sites, etc.

7. Prevention

Preventative security is an important part of ZoomInfo’s layered approach to security.

- ✓ Critical Assets
- ✓ Data Protection Layer
- ✓ Application Protection Layer
- ✓ Cloud Security
- ✓ Network Security
- ✓ End Point Devices
- ✓ Perimeter Defense
- ✓ Physical Protection

Key to our incident prevention strategy are identifying what data we need to protect, where that data resides, and who requires access.. Information assets include data that has value to our business, including business intelligence, customer data, passwords, keys, etc. Such assets are protected in part by appropriately provisioning access based on the needs of the specific job function or role.

7.1 DATA PROTECTION AND ENCRYPTION

Customer access is protected with Multi-Factor Authentication (MFA) and/or Single Sign On (SSO). Customer data is encrypted at rest using AES256 and browser client communication is encrypted with a minimum of Transport Layer Security (TLS 1.2). Passwords are stored with a SHA256 salted hash format.

7.2 NETWORK AND INFRASTRUCTURE

Our services are hosted on the three major cloud providers with hosting data centers in the U.S. Our use of automation throughout our operations minimizes the need for “human touch” to critical systems and data, further minimizing risk vectors.

Within these cloud providers we use multi-layered security from the layered application architecture and the firewall functions the cloud providers make available.

We also use third-party providers of Web Application Firewalls, internet facing protection, and DDOS protection, along with BOT. These services and our corporate environments are also protected with gateway devices with limited local computing services.

7.3 HOST AND END POINT

Our corporate systems are heterogeneous for the purpose of maximum productivity, and include Linux, Mac, and Windows. Critical systems are centrally controlled and monitored. End Point devices have layered security including state of the art malware and incident detection and response. End Point devices are patched at regular intervals along with operating system and applications updates.

7.4 PARTNERS AND VENDOR RISK

Our cloud services partners have strong security controls in place for managing all aspects of security and meet each of our rigorous requirements. They also provide security services for their user base allowing ZoomInfo to collect, manage, and respond effectively to alerted security events. These events can also be forwarded to the ZoomInfo Security Information Event Management (SIEM) tool for analysis and investigation as part of ZoomInfo's Cyber Security Operations Center.

We have a full risk assessment program in place to review prospective vendors. The vendor risk assessment includes evaluating the risks each vendor poses to us and, based on that assessment, outlining mitigation efforts on vendors that complete the process.

7.5 IDENTITY AND ACCESS CONTROL

Single sign-on and multi-factor authentication are used extensively throughout ZoomInfo. Testing and production systems have additional, highly granular controls to ensure that only approved access is granted. Nevertheless, we also have extensive monitoring, logging, and anomaly alerting for access and related activity. Application and system controls are subject to independent audits on a rotating basis.

Access is driven by either the on-boarding process or an individual request through the helpdesk ticket system. Access is validated based on the request being approved by either the application or system owner or the user's manager.

7.6 SYSTEM DEVELOPMENT LIFE CYCLE AND APPLICATION SECURITY

ZoomInfo applications are designed, developed, and deployed including processes and workflows, with security in mind at each step. This 'Security First' mentality continues into the application within the cloud production environment. In design, the Cloud Security Alliance and ISO principles are applied as needed. In development, both new code and modified code are subjected to dynamic security testing and static code analysis prior to being promoted to production. In deployment, both regular and ad hoc internal and third party penetration testing is performed to detect and mitigate vulnerabilities.

ZoomInfo has multiple protections in place between the user's browser and our applications, to address potential attacks before they ever reach our environments. A dedicated fraud and abuse team monitors for anomalous application access or usage.

Our Continuous Delivery and Continuous Deployment (CI/CD) systems are built on a software-defined infrastructure. When human intervention is required, activity is logged and monitored for additional protection against any possible insider threat.

Developed code is put through a standard automation process after it has been thoroughly vetted by our QA, DAST and SAST testing, user acceptance, and security reviews. Access to automation systems is tightly controlled and limited to a select few staff whose roles require access and authentication. All this access and activity are logged.

7.7 MALWARE

All systems, from a user's system to our production servers, are protected with a best-in-class endpoint protection system that looks for known malware and monitors for malware typical behaviors. These systems report to a central monitoring portal and alert or block unusual activity. Any system showing anomalous behavior can be remotely disconnected from the network to prevent lateral spread.

7.8 PHISHING

Like many organizations, ZoomInfo is continuously targeted by phishing attacks.   To reduce the risk of a successful attack, we continuously test employees with mock phishing campaigns, to identify weaknesses and raise and maintain awareness. Failing a campaign requires one to attend additional focused training sessions. Phishing is an area of focus in our mandatory information security training programs.

7.9 PHYSICAL

Our corporate offices employ appropriate levels of physical security, including badged, monitored, and secured entry.

As to our system infrastructure, each of our cloud service providers employs best-of-breed physical security. The physical media underlying the cloud service is handled by the provider, at their data centers, on their physical systems, and protected by extensive security and process controls that provide a very high level of data security.

8. Detection

ZoomInfo has anomaly detection layers and tools in place to catch potential threats before they can exploit our environment.

8.1 THREAT DETECTION AND ANALYSIS

Defensive layers at the edge include Distributed Denial of Service (DDOS), Web Application Firewall (WAF), Firewalls, Network Intrusion, Intrusion prevention, OWASP based filters, Access Control lists (ACL), and agents on endpoint nodes. All these feed into centralized management, where alerts are automatically and/or manually addressed, and threats suppressed.

8.2 LOGGING AND MONITORING

ZoomInfo has extensive logging in place for performance, operations, and security related events. Logs are held for 90 days for most systems and stored where necessary for a year. Dedicated teams are responsible for monitoring and reacting in a timely manner to events such as anomalies, service degradation, or security incidents.

For events that are not the norm, ZoomInfo has a formal incident management process with training and testing for this team being held. These include callout processes or simulation events.

8.3 FRAUD AND ABUSE DETECTION

ZoomInfo also has a dedicated fraud and abuse team continually observing defined thresholds for application activity to detect and report unwanted action in real time. Using custom-built tools, this team of application and product management experts respond to events in real time to prevent and respond to anomalous activities.

9. Response

ZoomInfo has well-defined response plans to address different events at the appropriate level within the organization.

9.1 INCIDENT MANAGEMENT

The Global Incident Response Management process outlines our response if our production services are impacted. This process is for managing an incident and is formally defined. If the impact is beyond that of the defined incident, the Global Crisis Management process is initiated as discussed below.

A thorough process enables quick response from the incident management team that can engage the right incident response teams. The process outlines concise steps required to initiate and manage the incident, as well as post-incident, process maintenance, and root cause analysis protocols.

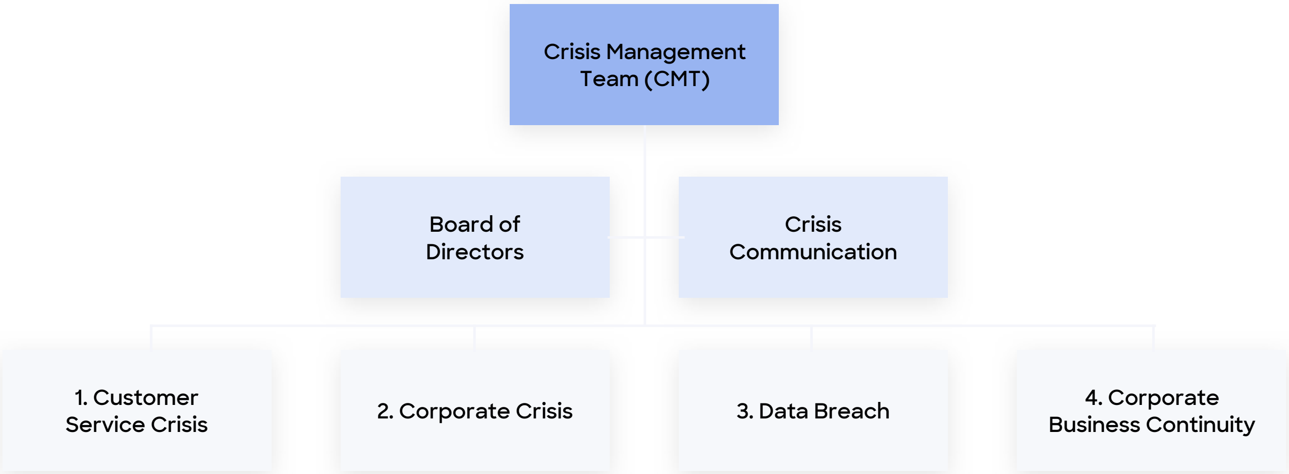
Successful incident response relies on more than simply detecting and responding to security incidents. ZoomInfo's incident response program is built on assessment, plan initiation, containment, eradication and recovery, and post-incident activities. These are supported by plan maintenance activities, including, training, testing, and simulation.

9.2 CRISIS MANAGEMENT

The Global Crisis Management process outlines our response to certain events that could have a significant impact on our employees, customers, investors, or the general operations of the company, including service interruptions, reputational harm, shifting market forces, or change in governmental policy or regulation.

The process outlines concise steps required to initiate and manage the crisis, including post-crisis, process maintenance, and root cause analysis protocols.

ZoomInfo addresses crises by defining a formal process. The overall responsibility for any crisis resides with the Crisis Management Team ("CMT"). The CMT manages all types of crises including corporate crises, data breaches, customer crises, and business continuity issues.


Crisis Management Team (CMT)
Board of Directors
Crisis Communication
1. Customer Service Crisis
2. Corporate Crisis
3. Data Breach
4. Corporate Business Continuity

9.3 BCP/DR

We currently take many steps to create a redundant and robust infrastructure and application environment. This includes offices, third party service providers, robust cloud providers with multiple high availability zones, data backup and retention processes, and more. Since ZoomInfo is a 100% virtual SaaS offering, we have the ability to swiftly address any degradation of service and quickly restore to normal levels, with an uptime of greater than 99.9% year after year.

10. Remediation

ZoomInfo takes a proactive approach to security and quickly addresses risks. When a weakness is found, a risk review is performed, a risk level assigned, and the risk addressed with a priority based on impact.

10.1 VULNERABILITY AND PATCH MANAGEMENT

To maintain a secure environment, ZoomInfo has an established vulnerability testing schedule, with results reported into our Agile task tracking software, assigned a criticality and priority, and addressed through our development life cycle processes.

10.2 RISK TRACKING

In addition to managing risk through established protocols and processes, we also maintain a risk register to capture actual or potential risks not amenable to discovery through automated methods. Entries here are reviewed by executives for relevance, potential severity and risk, and acted upon accordingly.

11. Certification and Controls

ZoomInfo has multiple certifications, attestations and compliance which is monitored and managed by our Governance Risk and Compliance (GRC) team.

11.1 CONTROLS

In accordance with the values promulgated by ZoomInfo's Board of Directors and senior management, ZoomInfo's primary objective in its approach to internal control is to provide reasonable assurance that its controls are suitably designed, implemented, and operating effectively to meet system, security, and compliance requirements. The control structure is focused on ensuring that assets are protected from unauthorized use or disposition, and that processes and procedures are in line with our strategic goals and are executed with senior management authorization.

All network, system and application aspects are regularly scanned, and any critical vulnerabilities are addressed upon discovery.

11.2 CERTIFICATIONS AND ATTESTATIONS

ZoomInfo is ISO 27001 and SOC 2 Type II certified.

12. Contact Us

Contact us regarding security related questions through our sales representatives, or your account manager if you are already a client. Any questions on security sent to them will be routed internally and they will reply with the answers.

Should you need to contact us regarding an actual or potential security issue, such as receiving a phishing email purporting to be from ZoomInfo, bugs, or any other security concern, please let us know by contacting us at Security@zoominfo.com, and thank you in advance!