CoBro Data Security Protocols and Security Breach Plan
February 22, 2019

Assurances data is stored domestically.

CoBro Consulting client primary data is stored on Microsoft Azure Cloud: SQL Databases, terminal server, and web server located in United States (West and West Central US). CoBro disaster recovery data, SQL Databases, is replicated to West Central US; terminal server and web server are replicated to East US. Server monitoring, data maintenance, management, security and daily backups are performed by Microsoft Azure monitoring and warning systems; DataDel LLC, San Diego based company and CoBro Consulting staff.

Security Protocols

CoBro Consulting hosts all client data on Microsoft Azure Cloud. Data is encrypted at rest and in transit. All confidential data processed, stored, and/or transmitted by CoBro is maintained in a secure manner that prevents the interception, diversion, or other unauthorized access to said data. All of our computer systems and servers require the use of secured passwords to access computer databases used to store or transmit the data. We implement secure practices for assigning passwords and encrypting data to maintain the integrity of the systems used to process, store, or transmit data provided under our contract agreements. Additionally, all CoBro staff (employees and subcontractors) are required to execute a confidentiality statement, which requires them to maintain the confidentiality of all program participant related personally identifiable information. Moreover, all CoBro staff are periodically required to complete relevant online cybersecurity courses which contain end-of-course tests they must pass.

Additionally, Microsoft Azure Cloud is our Data Center Provider. CoBro Consulting technicians follow Microsoft Azure FERPA Implementation Guide to set up their cloud network, data storage, back ups, and disaster recovery processes. Detailed information can be found at the following website: https://gallery.technet.microsoft.com/Azure-FERPA-Implementation-441b6b71 . The FERPA Implementation Guide for Microsoft Azure whitepaper provides insight into how Microsoft meets its compliance obligations on the platform and presents best practices and security principles that are aligned to the Family Educational Rights and Privacy Act, International Organization for Standardization (ISO) 27001, Microsoft's Security Development Lifecycle (SDL), and operational security for online security.

CoBro technicians perform a weekly vulnerability scan via the Azure Security Center. At the conclusion of each scan, a security status report is generated that also includes suggestions regarding steps we can take to make our cloud services even more secure as technology advances and more cyber security tools and strategies are developed. To this end, CoBro technicians convene monthly meetings to determine appropriate additional tools and strategies for implementation.

In terms of our CoBro staff handling of client data, procedures and systems are in place to ensure all participant records are kept in secured facilities and access to such records is limited to CoBro personnel who are authorized to have access to the data. Our staff maintain the confidentiality of individual data records at all times while such information is in their possession, and only the assigned research staff have access to personal identifying information for the purpose of preparing, formatting, analyzing, and/or reporting on student data for program evaluation purposes. All discussions, deliberations, records and information generated or maintained in connection with these activities are not to be disclosed to any unauthorized person.

All client data hosted and secured by CoBro Consulting is owned by that client. At the end of our contracted work with each client, we provide the client the opportunity to safely download all of their data maintained by CoBro, using secure https download processes. For audit documentation purposes, our policy is to maintain such data for three years after contract expiration for each client, unless otherwise specified by each individual client. After the three years, all client data maintained by CoBro Consulting is professionally destroyed, using industry standard procedures.

Data Breach Protocols

According to the California Information Security Office Incident Reporting and Response Instructions (SIMM 53-40A May 2016), the following situations meet the criteria as a "data breach incident requiring notification" for state entities.

"An incident is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Incidents which must be reported to the California Information Security Office (CISO) and the California Highway Patrol (CHP) Computer Crimes Investigation Unit (CCIU) immediately following discovery include, but are not limited to, the following:

1. State Data (includes electronic, paper, or any other medium)-

a. Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal.

b. Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.

c. Deliberate or accidental distribution or release of personal information by a state entity, or its personnel in a manner not in accordance with law or policy.

d. Intentional non-compliance by the custodian of information with his/her responsibilities.

2. Criminal Activity - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502.

a. Unauthorized Access - This includes actions of state entity personnel and/or unauthorized individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems.

b. Attacks - This includes, but is not limited to, successful virus attacks or exploited vulnerability, web site defacements, and denial of service attacks.

3. Equipment – This includes theft, damage, destruction, or loss of state-owned Information Technology (IT) equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.

4. Inappropriate Use – This includes the circumventing of information security controls or misuse of a state information asset by state entity personnel and/or any unauthorized individuals for personal gain, or to engage in unauthorized peer-to-peer activity, obscene, harassing, fraudulent, illegal or other inappropriate activity

5. Outages and Disruptions – This includes any outage or disruption to a state entity's mission critical systems or public-facing web applications lasting more than 2-hours, or in which the incident triggers the state entity's emergency response or technology recovery.

6. Any other incidents that violate state entity information security or privacy policy."
CoBro Incident Response Team

If a data breach meets any of the above criteria, it will be the responsibility of the CoBro Consulting Incident Response Team (IRT) to initiate and comply with the established CoBro Cyber Breach Response Protocols. Designated IRT members are as follows:

- Escalation Manager: Darlene Cole
- Program Manager of the program or office experiencing the incident or breach: Urban Pelicon or Keren Brooks, depending on location and type of the breach
- Information Security Officer (ISO): Urban Pelicon
- Chief Privacy Officer/Coordinator (CPO) or Senior Official for Privacy: Keren Brooks
- Public Information or Communications Officer: Darlene Cole
- Legal Counsel: Harry McGahey, esq.
- Technical Expert: DataDel, LLC (Delfin Esposo) and CoBro Consulting, LLC (Urban Pelicon, CIO) representative, depending on the nature of the breach
- Other CoBro personnel, as appropriate, given the nature of the breach.

Note that the Escalation Manager, often the ISO or CPO, is responsible for ensuring appropriate representatives from across the organization are involved and driving the process to completion

Notification Process

The CoBro Consulting designated CPO will immediately report any actual or suspected incident meeting the criteria described earlier or breach of personal information to the CA Department of Justice Attorney General using the form at the following site:

https://oag.ca.gov/privacy/databreach/reporting

The Communications Officer will similarly immediately (within eight, 8, hours) notify any and all CoBro clients impacted by any known or reasonably suspected unauthorized disclosures of confidential or personal data, or other similar breach.

Incident Response Plan

The following steps comprise our incident response (IR) plan regarding how CoBro principals and/or employees will address a serious data breach or malware incident.

a. Don't turn off the suspected computer. Turning off the computer might seem like the instinctual first step but often will destroy evidence and erase valuable clues that will allow a forensic expert to fully assess the attack.

b. Contact law enforcement. Many local law enforcement offices have computer or e-crime sections that are experienced in investigating and helping with these types of attacks.

c. Document the potential scope of the breach. Establish current facts about the breach and communicate them as appropriate. These facts may include why a breach is suspected, the number of systems accessed, and the data that may have been stolen. Executives will be kept apprised of the facts as they evolve, measures taken to date, measures that will be taken, and what to expect going forward.

d. Determine notification requirements. This includes identifying, assessing, containing, remediating and reporting a breach. Determine if outside help is required. Questions to consider include whether CoBro has the capabilities to respond to the incident internally and whether we need to engage a forensic investigator, an IT security professional, and/or expert legal counsel.

e. Determine notification requirements. Retain system, application, database and network device logs and avoid making changes to the system suspected of being compromised before data is preserved. This may involve consulting with an expert to assist CoBro in acquiring a forensic image of the hard drives and live memory of the systems suspected of being compromised and following proper chain of custody procedures.