GoodCorp Audit Notes
Leadership

- While we do not have a formal security program, the executives are focused on improving organizational security.
- Executive leadership wants to handle security issues internally given the sensitive nature of our client space.
- Interviews are underway to hire Chief Information Security Officer and subsequent management personnel to round out the team.

Business Risks

- Selling systems that provide management of customer's sensitive data to include government customers has made it apparent that we need better security.
- Leadership is concerned we will not be able to detect an attack and even if we do, what do we do then?
- Due in part to threat information that was shared with GoodCorp by the U.S. Government, it was initially assessed that GoodCorp would be a likely target of organized crime and Nation-State threat actors.
- GoodCorp is in the beginning stages of defining that risk and this assessment is a part of that overall strategy.
- Executive leadership is unaware of what level of risk the organization can or should accept in relation to our customers and products/services.

Asset Management

- The organization purchases mobile devices for some employees and tracks those in an inventory, but many users use their own mobile device which are not tracked.
- There is not a formal process for managing systems. The organization is aware of who has provided devices and can locate those devices. They do not have a current program to track personal devices.
- Users are afforded the ability to install applications as they need them. Most of our employers are software developers and they need access to be able to use the best technology on their projects.
- The organization tracks its licenses for approved applications but does not have a comprehensive list of all approved software and what is installed where.
- The organization does not have any documented systems or communications flows other than basic firewall and configuration rules.
- GoodCorp uses its proprietary solution, CDMS to manage its data and files. CDMS has multiple policies and features for managing, classifying, handling data.
- GoodCorp has documented a loose outline for its critical workforce and the beginnings of an Incident Response policy is being drafted.

Business Environment

- GoodCorp does know where it sits in the supply chain with government and other customers and has identified it is a potential target.
- The organization does have an overall mission objective to continue to provide CDMS to its customers and the Security program's role in this vision is still being outlined.
- GoodCorp has identified some critical components to its services, however much of the knowledge of what systems and dependencies play into this have not been documented.
- GoodCorp does not have a Continuity of Operations Plan (COOP) but plans to include this in its Incident Response policy that is currently being drafted.

Governance, Risk Assessment & Management

- Goodcorp is in the process of creating a cybersecurity policy that follows the Cybersecurity Maturity Model Certification (CMMC) as prescribed by the government.
- The processes following CMMC are on an ad-hoc basis and have not been fully documented or standardized.
- Goodcorp does not currently have a Vulnerability Management program. All vulnerabilities are submitted from external tests from customers or internally reported.
- The organization does not have a Cyber Threat Intelligence program and receives all reports from news articles.
- While GoodCorp recognizes that it is potentially a target for APT and organized crime groups, there is no documentation to outline these threats.
- The HR department does not have a standard onboarding/offboarding procedure for all employees. Many ex-employees may still have access to unknown systems.
- GoodCorp is in the process of creating a Risk Management plan which will be reviewed on an annual basis.
- GoodCorp does have a security questionnaire that is sent to all of our partners to identify partner risk. However, there is no standardized process.

Users and Training

- Users receive annual training on data privacy, HIPAA compliance, general Personal Identifiable Information data handling practices.
- Users can bring in personal mobile devices and connect to the office Wi-Fi.
- Users can take home their work laptop to work remotely on occasion.
- Users can access email, calendar, company data and other communications tools via their mobile devices
- Many of the users in the network have some form of elevated privilege or administrator access to complete their assigned work.
- As most of the users work on the same project, there is no segregation in the network regarding access to systems and resources. This also means that non-developer roles can potentially access these services.
- We do use Windows Active Directory to manage authentication on the network to resources, but we do not have a formal process for managing users, their roles, and associated accesses. Currently, users just ask for something and it is reviewed manually.

Data Security, Maintenance & Protective Technology

- GoodCorp uses their proprietary solution CDMS to manage all GoodCorp's data and files.
- CDMS provides integrity of files through hashing and privacy through encryption of data in transit and at rest.
- CDMS keeps historical copies of data in case of data loss.
- CDMS has multiple policies and features for managing, classifying, handling data.
- Due to developer autonomy, there is currently some customer data held in staging/QA environments with no data leak prevention controls in place.
- GoodCorp does have a System Development Life Cycle (SDLC) policy that is loosely adhered to.
- Changes to our processes are on an ad-hoc basis.

Security Monitoring & Detection

- The organization is using Security Onion to trial the use of it as a production SIEM and planning on deploying Wazuh agents soon to monitor the hosts in the network.
- Our CDMS has limited security baked into the development process. Code is pushed to our code repository and every night the code is compiled and ran through a scanner to assess if there are any bugs or known vulnerabilities in the code.
- We do not have a formal security operations team. The goal of this assessment is to analyze where we are and understand what each of the controls means as it regards to prioritizing funding and efforts.
- We have had an outside firm come in last year and run a vulnerability scan. We patched numerous critical vulnerabilities and on their second scan, we had no high or critical vulnerabilities in the network.
- Discussions are underway to get an external company that handles incident response on retainer in case something happens while we mature our program.