Cyberdyne Systems

Memo- Request for Proposal

RE: Server, Desktop, and End User Device Security Analysis Required

11/1/2025

Potential Vendor,

On behalf of Cyberdyne Systems management review committee, we are extending this request for proposal document to outline Cyberdyne's intent to engage outside assistance in an analysis of our server, desktop, and end user device-based systems. You will find our project's requirements listed below.

Summary and Background-

Cyberdyne systems is a California based manufacturer of microprocessors, microcomputers, artificial intelligence, and robotics-based technology. Cyberdyne currently employs four hundred technicians, engineers, sales, management, HR, administration, and information technology resources, operating out of a multi-building campus. Cyberdyne has two locations, one in California and one in Taiwan. All day-to-day administrative, research/development, sales and accounting operations occur in the California campus, while production of Cyberdyne hardware products occurs in the Taiwan location.

Project Scope-

The goal of this analysis is to identify security related issues with Cyberdyne's systems across the two locations and Cyberdyne's work force. Cyberdyne is requesting that potential vendors (You) review the attached information that has been supplied internally to create an analysis report that will outline and include the following:

1. Introduction/Executive Summary for our management team about the scope and purpose of the report.
2. Current observed practices and issues
3. Potential controls for identified practices and issues.
4. Potential policies for identified practices and issues.
5. Potential training plans for identified practices and issues.
6. Final summary outlining how your plan will deliver a multilayered approach to protecting our systems and users.

Identified Areas of Improvement-

As identified by our management teams, various departments, and end users, the following are some of the reported issues, as well as practices that occur on a regular basis within Cyberdyne. They have been broken down into categories below:

Devices-

- Users have reported slow and sluggish experiences while accessing systems in their various locations.

- Users report issues while trying to collaborate with company systems, as instructions and direction on specific use seem unclear.
- Devices are often lost or reported stolen, with inconsistent replacement devices being issued.
- Laptop devices often travel back and forth from the Tiawan factory to the California location, and vice versa.
- Data on devices can contain sensitive or confidential information.
- Cyberdyne sales team often employes workers that primarily work from home and require remote access to Cyberdyne's California systems.
- Devices in the Tiawan based location often encounter interference from surrounding locations as they are in a densely populated industrial park.
- Cyberdyne executives require access to high priority systems but often use their personal machines for ease of use and personal preference.
- Users have reported issues and concerns regarding corporate antivirus solutions, as none is apparent.
- There are many resources, systems, and devices in use, but Cyberdyne is managing them locally, requiring end users to often remember multiple passwords and accounts.
- Users of times have issues accessing network and internet resources, as well, IT appears to have a challenging time managing access to the same resources.
- IT has reported issues with managing and deploying software, settings, and policy to end user devices.
- Cyberdyne's management, along with IT, would like visibility into network and device related information so it can help detect and monitor against threats.
- Passwords and accounts for devices are often shared and reused and not unique.

Employees-

- Cyberdyne has an extremely high level of turnover at both locations, with frequent hiring required.
- Due to the heavy turnover, users report exhaustion, dismay, and potentially negative attitudes towards the company.
- New employees have very little time to be on-boarded and brought up to speed in how aspects of the systems work, and what the rules are.
- Sales based employees work on commission.
- Often employees are repurposed or moved throughout the organization to fill gaps in understaffed departments.
- IT workers often suffer from a skills gap in picking up new technology and are versed in older systems but are tasked with deploying new systems with which they are unfamiliar.
- Managers' report having challenging times recruiting quality workers that stay with the company and often report that products from competitors seem to beat them on the market.
- With little training on devices and systems use, some employees have taken to using personal devices and or developing shortcuts for work.

*Customer Data***-**

- Cyberdyne AI and Robotics engineers often work with high volumes of collected customer data used in research and development of its tools.
- Cyberdyne also works as a vendor for many local and state governments, providing solutions, IT services, and sales of hardware and software.

Locations-

- Managers are often unaware of specific requirements for the regions they reside in for IT business practices.
- Data must securely be sent between the two locations and often is shipped via external devices or sent via email.

Additional Internal Resources-

In addition to the information supplied in the "Areas of Improvement" section, we have provided the following items to aid in your analysis:

1. **Memo- Request for Proposal (this document)**
2. Device Definitions Table
3. User Definitions Table
4. Regulatory links page
5. Final project powerpoint

We look forward to working with you to develop a plan to make Cyberdyne a safer and more secure place to work. Thank you for your time, and we look forward to your report.

Sincerely,

Dr. Miles Dyson

Director of Special Projects

Cyberdyne Systems Corporation