Baldwin Wallace University Information Technology Guideline

Issued by:	**Information Technology**
Title:	**Vendor Evaluation Research Tools**
Number:	**ITG-BW-16-02**
Publish date:	**July 17, 2019**

A. Evaluation Tools

The following are potential web sites to search for breaches and related information on vendors or products.

a. Check technologies for Known Vulnerabilities:

CVE® is a list of entries—each containing an identification number, a

description, and at least one public reference—for publicly known cybersecurity vulnerabilities. CVE Entries are used in numerous cybersecurity products and services from around the world, including the U.S. National Vulnerability Database (NVD).

https://cve.mitre.org/

b. Have I been pwned?

Check if you have an account that has been compromised in a data breach

https://haveibeenpwned.com/

c. Checking the Dark.net:

Check if that domain has experienced compromise by checking a few (or a number) email addresses. Concentrate on leadership emails.

https://spycloud.com/

d. Check for Data breach:

Check to see if that company has experienced a data breach.

https://en.wikipedia.org/wiki/List_of_data_breaches

e. Check for Data breach of privacy information:

Check to see if that company has experienced a data breach.

https://www.privacyrights.org/data-breaches

f. In-depth Cyber Assessment Tools:

Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment) to help institutions identify their risks

and determine their cybersecurity preparedness. The Assessment provides a repeatable and measurable process for financial institutions to measure their cybersecurity preparedness over time.

https://www.ffiec.gov/cyberassessmenttool.htm

g. Misc Tools:

The following is a list of free tools that can be used to test, perform vulnerability scanning, and assess technical solutions.

https://cyberx.tech/free-cybersecurity-tools/#nethardening