Western Technical College

Information Technology
Cybersecurity Summary

Current status on cybersecurity:

We know that we are attacked constantly, we have thousands of attempts from hackers each day. Following are actions that we have taken to assist our users in identifying attempts and work toward total safety of information at our organization:

- Internal/External notification flags on each email. Every email that is received from outside our organization is tagged with a color-coded flag to alert users that it is not an internal communication.

- Multi-Factor Authentication – we are turning Multi-Factor Authentication on for our network this year. We have hired a security person for our active directory team this quarter. We already use multi factor authentication in several of our other applications, such as Greenshades, one of our HR payroll and leave systems. We have several options for authentication such as text, call and using the Microsoft Authenticator Application.

- We use a secure transfer option, (https://dropoff.westerntc.edu) to transfer documents which have PII in them. It is very simple to use, and can be used internally, and externally to our organization. This is available to all Western users and can be used by our stakeholders to transfer items to Western users.

- Personally Identifiable Information (PII) – we are actively blocking PII from being emailed. We have a data loss prevention (DLP) policy enabled in discovery mode to determine current usage. The policy enables notification for what it determines as a medium level event (1-9 pieces of PII in an email) to remind users to use the new sensitive data transfer process. The DLP tool blocks anything that is considered a high-level event (10+ pieces of PII). We constantly scan for existing PII and alert users if we find anything. We periodically review the DLP policy notification list to send reminders and check progress towards reduction of PII in our email system.

- To minimize risk, we are actively deleting old email – we set up a policy to clean up deleted items that are older than 30 days. When we scanned our system, we found many mailboxes with large amounts of data in that folder that broadened our exposure, we actively delete this old email currently.

- Training and education – every user must take a cyber-risk course from our training partner on an annual basis to keep safety first and foremost in our daily activities.

- We added a reporting button in our email system for ease of reporting for our users in the event they received a suspicious email in the second quarter of 2019.