CISO Annual Report 2023

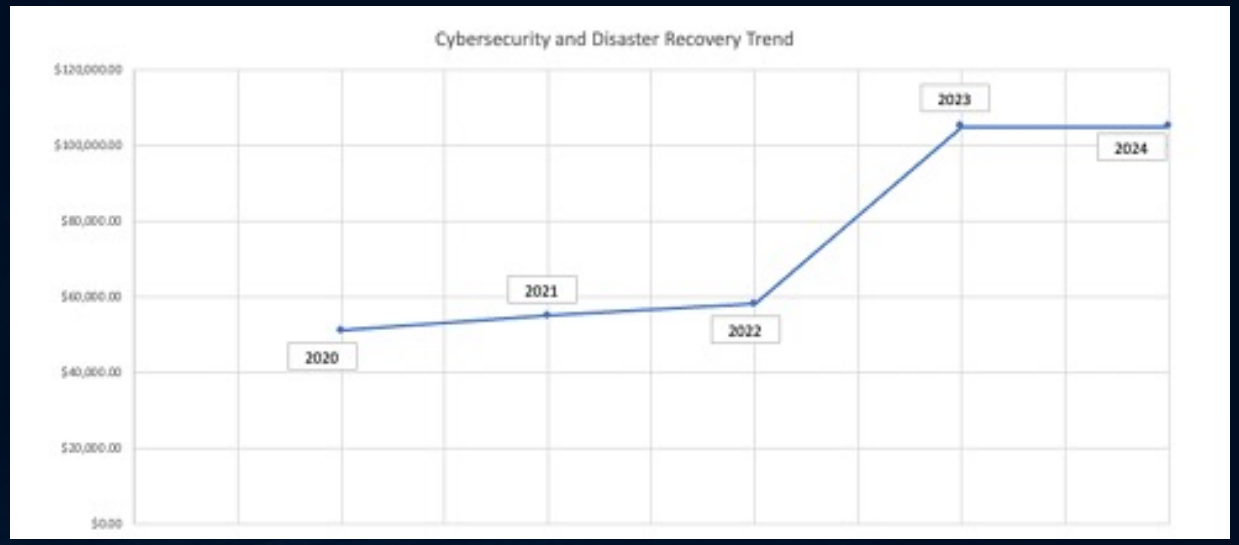
WILLIAM MANN, CGCIO
BOROUGH OF WEST CHESTER

This presentation includes highlights from the CISO Annual Report.
The report is available for anyone who would like it.

INTRODUCTION

- Information Technology Services are the backbone of our organization. It is through our coordinated and connected infrastructure, software (both small and enterprise) & hardware solutions that we remain productive, collaborative and secure.

- Because of our reliance on connected services, cybersecurity challenges continue to require attention and are now a daily, if not hourly responsibility.



INTRODUCTION

- The information technology department continues to adapt and change with both the national technology landscape and the needs of our organization. While services relating to enterprise applications and data management have shifted, our cybersecurity efforts have equally grown, requiring the need for continual attention, management and response.

- The physical infrastructure of our organization also continues to expand. Our physical infrastructure includes **virtual hosts**, **servers**, **firewalls**, **VPN's**, **backup appliances**, **video & security services**, **audio-recording and streaming**, **network switches**, **access points**, **cameras**, **computers**, **mobile devices**, **digital document servers** and more. All these physical appliances require management, care, and monitoring.

PROJECTS - *projects led CISO*

- **New Virtual Hosts**
  This project saw the replacement of our 3 virtual host servers with new ones that will have a life span of 5+ years. These host appliances are where are servers are maintained. A second host acts in a redundant compacity while a third acts as our managing appliance.

- **Acoustical Treatment**
  This project saw the installation of acoustical treatment panels in the Borough Council Chambers. This is a project where the cope was downgraded, saving about $26,000 in capital costs.

- **Expanded Multi-Factor Authentication**
  This project saw the upgrade for many of our users to DUO, away from Microsoft Authentication for two-factor service. This new service, in addition to protecting our cloud services with two-factor authentication protects our organization on a domain (network) level as well.

CISCO DUO

PROJECTS - *projects led CISO*

- **Website Refresh**
  As part of our three-year contract renewal with CivicPlus we were able to fresh and redesign much of our website.

- **Expanded Disaster Recovery Services (DATTO)**
  This project saw the replacement of our (at the time) existing onsite and remote backup service (Axcient) with DATTO. DATTO brings more efficient and expanded onsite and offsite disaster recovery services.

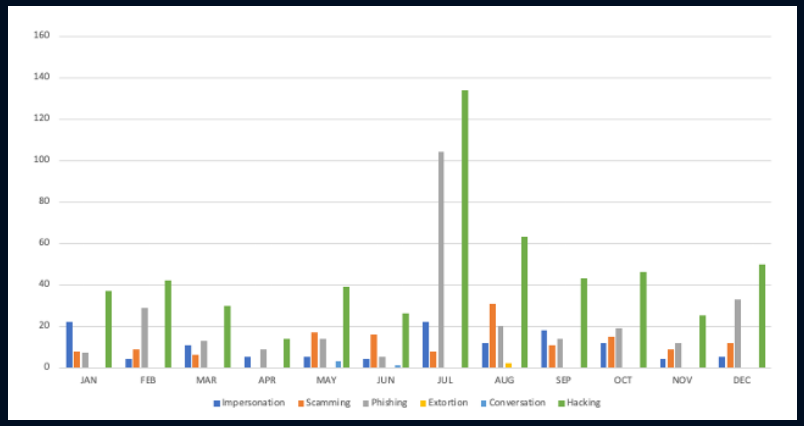
- **Expanded Cybersecurity Services (Barracuda Data Inspector)**
  This brand-new service from Barracuda is one that we wanted to invest in right away. This new service looks for and flags PII (personal identifiable information) on a user and administrator level. We are still working with Barracuda on layering this solution into our system and workflow.

PROJECT ASSISTS – *projects led by others*

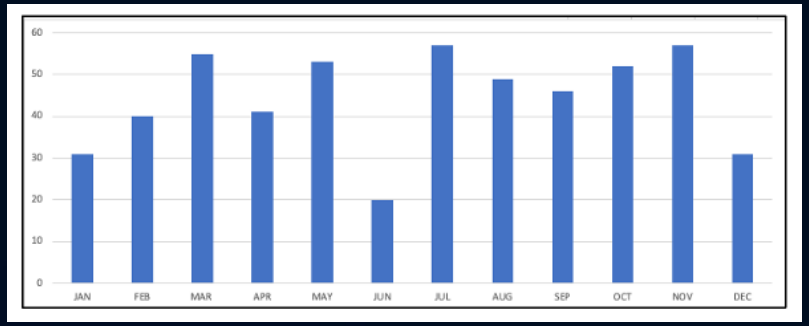
- **Cartegraph**
  Project Lead: Nick Fink, Data Analyst and Enterprise Applications Manager
- **Brightly (SmartGov)**
  Project Lead: Nick Fink, Data Analyst and Enterprise Applications Manager
- **Flash – Parking Kiosk System**
  Project Lead: Ramsey Reiner, Parking Services Director

CYBERSECURITY MANAGEMENT

- **Impersonation Protection (phishing, scamming & impersonation)**
  - There were **549** automated cybersecurity email threats flagged and prevented during the year. Each of these requires the information technology staff to stop and double check the legitimacy of the threat and make sure that nothing related was delivered.



- **Incident Response**
  - This year we manually investigated and remediated **532** email threats. Many of these were reported by our staff while others were isolated by the information technology staff.
  - **These self-reported incidents demonstrate the importance of regular cybersecurity awareness training for staff.**



CYBERSECURITY MANAGEMENT

- **Account Takeover**
  - An account takeover is where a threat actor attempts to access or login to one of our accounts. This occurred **1** time this year.

- **Disaster Recovery**
  - This year we continued our disaster recovery services including three tiers of protection.
    1. On Premises (DATTO)
    2. Cloud Services (DATTO)
    3. Cloud to Cloud Backup Services (Barracuda) *Microsoft 365 services

CYBERSECURITY MANAGEMENT

- **Data Inspector**
  - This year we added Barracuda's Data Inspector to our cybersecurity environment. This solution monitors Microsoft 365 data for PII information.

- **Cybersecurity Awareness Training**
  - This year we provided **cybersecurity awareness training** to staff two times.
    - these training sessions were recorded and are available on our YouTube channel.
  - We continue to publish the **Cybersecurity Friday** newsletter.
  - We continue to test & educate staff with monthly phishing campaigns.

December 22, 2023 | Issue 71

Cybersecurity Friday

phishing - scamming
impersonation - viruses - trojan horses
malware - oh my!

staying cybersafe one week at a time

This Week on "Cybersecurity Friday"

This is our final special holiday cybersecurity themed issue of "Cybersecurity Friday. Next week, it's back to normal.

This issue we continue our coverage of holiday themed Cybersecurity themed tips, tricks and rules to live by to keep your information and the information of your organization secure.

Remember that all of the skills we learn during the holidays are just as important all year long.

Next week we will take a rare break for the Christmas holiday and then it's off to 2024!

-Bill

Cybersecurity All-Stars

This week's Cybersecurity All-Stars is everyone. This month's phishing test was a great success! Out of 120 users, no one (not one) interacted with the message and many of you took the extra step to report it to the IT Department. Not a single person fell for the fake training message, even

CYBERSECURITY AWARENESS MONTH

- Since 2004, the President of the United States and Congress have declared October to be **Cybersecurity Awareness Month**.
- This year's campaign theme was **"Staying Safe Online"**.

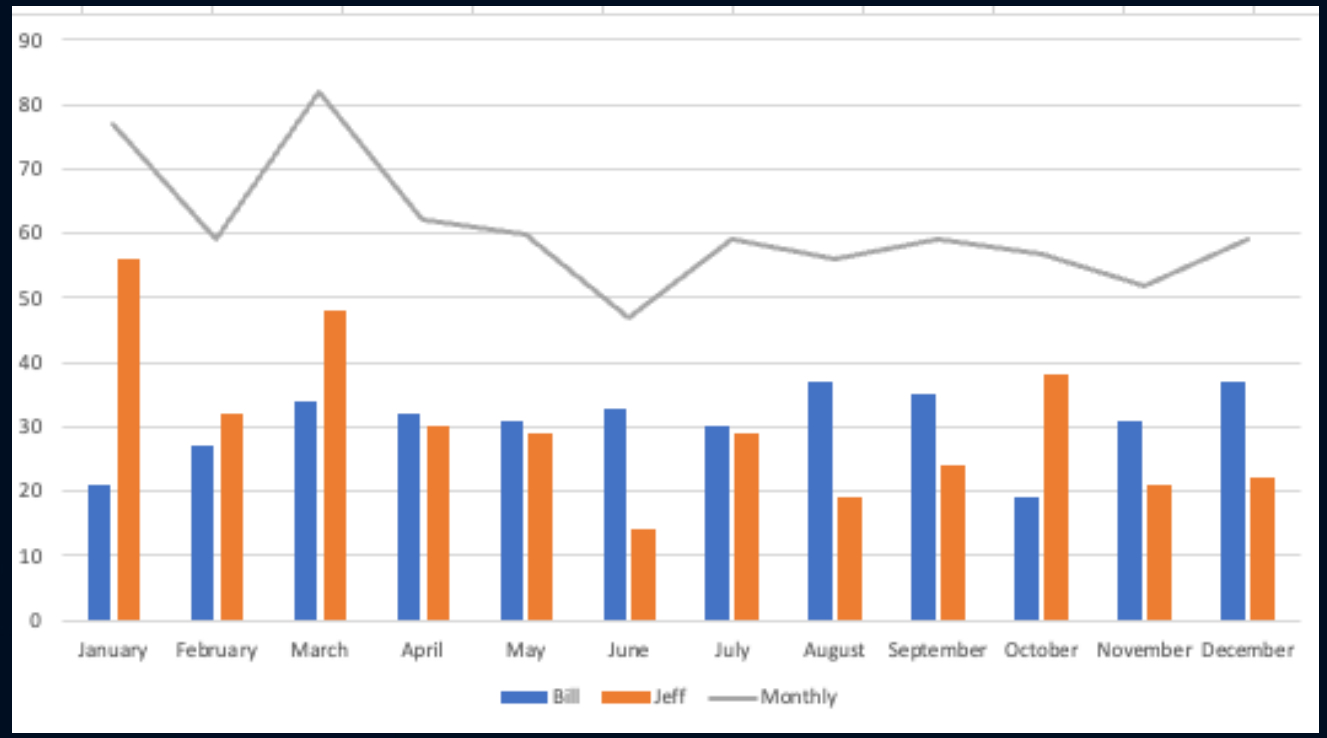
During the month we provided 4 ways you can stay safe online. Each weekly topic was covered as part of our Cybersecurity Friday Newsletter.

•Week 1: Using Strong Passwords Password Manages
•Week 2: Multi-factor Authentication
•Week 3: Updating Software
•Week 4: Recognizing and Reporting Phishing

HELP DESK SERVICES

One of the core duties of the information technology department is **help desk services**. It is through this day-to-day service that the information technology department interacts with the staff and provides support so that everyone can achieve their mission through technology services.

It should be noted that **help desk tickets only account for an estimated 70% of the total services** provided to staff.



Total Help Desk Tickets - **729**

UNSCHEDULED EVENTS

These are events relating to hardware and network services that the information technology staff responded to, outside of normal help desk, cybersecurity, and project related services.

- There were a total off 11 unscheduled events ranging from firewall failures, camera & security services, environmental services and more during the year.

SMALLER & UNPLANNED INITIATIVES

There are many tasks, large and small that are assigned to the Information technology Department that are **outside the scope of Help Desk Tickets and Projects**.

These activities are documented in the monthly CISO reports. There are too many of these to document in this annual report.

This year between August 1 and November 4, I successfully completed the **"High Performance Leadership"** course provided by the Professional Development Academy.
This course included 3 days of class work each week, 1 day in a small breakout group (I hour) of 12 other local government leaders and a 5th day in the entire class with 70+ local government leader

CONTINUED EDUCATION

Cybersecurity and technology in general are continually evolving and one of the best ways to remain ahead is through engagement, education, new ideas and dialog with other professionals in the same sector

1. **CGICO Recertification (2023-2026) -** *CompTIA and Rutgers* Universi**ty**
2. **Cybersecurity and Ransomware and Its Impact on Law Enforcement,** ***FBI***
3. **AZ-04000: Automating Administration with Power Shell,** *Microsoft*
4. **Cybersecurity Simulation – A Ransomware Attack,** *NACO and PDA*
5. **SC-0900T00: Microsoft Security Compliance & Identity Fundamentals**
6. **Leading on Purpose -** *Professional Development Academy*


CompTIA Public Technology Institute
and
Center for Government Services Rutgers University
Certify that
William Mann
has successfully been recertified for the
Certified Government Chief Information Officer Program
through July 28, 2026

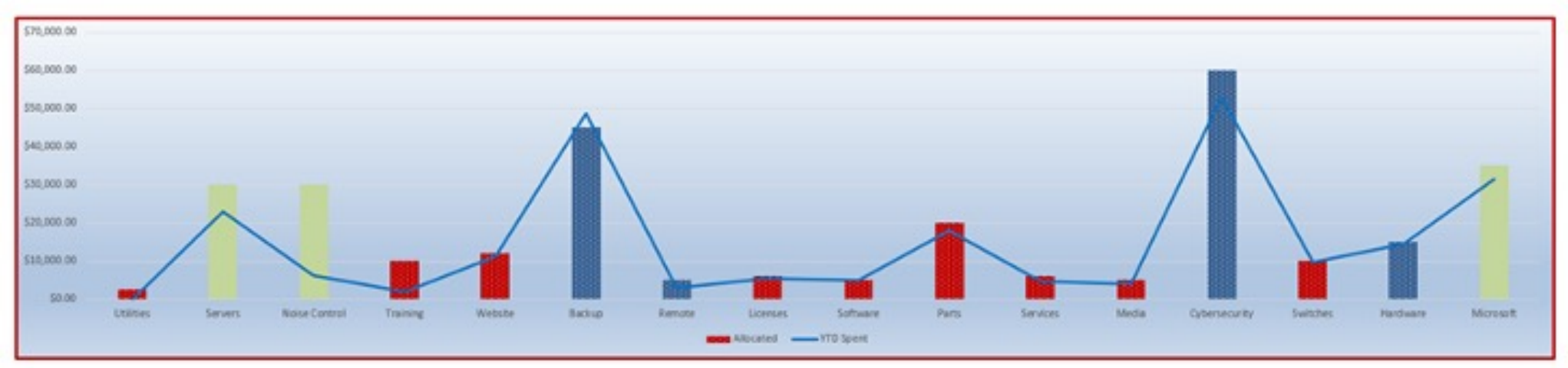

Leading On Purpose
Master Certificate
William Mann

This year between August 1 and November 4, I successfully completed the **"High Performance Leadership"** course provided by the Professional Development Academy.
This course included 3 days of class work each week, 1 day in a small breakout group (I hour) of 12 other local government leaders and a 5th day in the entire class with 70+ local government leader

INFORMATION TECHNOLOGY BUDGET

The 2023 budget included operations and capital expenses. We worked diligently managing costs and making sure that budget expectations are met. As part of our monthly process in the IT Department, we reviewed spending up to that point as well as looking ahead, projecting costs. The below graph displays the information technology line items, including capital expenses and where spending is up the moment of this report.

The below graph displays spending trends and status as of this report. The annual budget trended as expected.



William Mann, CGCIO
Borough of West Chester
wmann@west-chester.com