Background

- 1999: Started my career in the Office of Budget and Financial Planning as an Information Technology Specialist
  - Responsible for Desktop Support and Server Support
  - Financial and HR Reporting
  - Systems Development
- 2005: Hired as the founding director of Business and Management Systems (BAMS).
  - In the 16 years since, BAMS has grown to 11 employees
  - Increased responsibility to all C-suite Executives

Background - *continued*

- Responsible for 25+ departments including Office of Audit Risk and Assessment, University Legal Council
- In the past year, merged with IT Operations department and have additional oversight of departments like Police, and Power Plant
- Oversight of e-discovery program
- Oversight of our IT security program for those offices
- In my 20+ career, IT security has always been a part of my job
  - Masters degree in IT with a focus on IT security
  - Various SANS and other security training

Topics Covered

- University policies and standards
- Departmental standards
- Tools
- Compromises
- Covid
- Post-Covid and remote workforce

Distributed IT Security Program

- Philosophy for IT security at our university has always been that IT security is local and the network should be considered hostile (Zero Trust Network)
- Responsibility is bottom-up. Enforcement is top-down. All security is local.
- Philosophy of IT security being local will translate well with remote workers
- *A survey*

Standards/Policies

- Our CISO and Division of IT sets the policies and standards
- For the purpose of what we talk about today most is based around our University's minimum IT security standard.
- Our minimum-security standards are mapped to the 20 CIS Critical Security Controls.

CIS Top 20 Controls

- https://www.cisecurity.org/controls/cis-controls-list/
- A prioritized set of best practices created to stop the most pervasive and dangerous threats of today.
- Developed by security experts from around the world
- Refined and validated every year.

Minimum security standards

- Patching
- Inventory
- Firewall
- Credentials and Access Control
- Two-Factor Authentication
- Equipment Disposal
- Sysadmin Training
- Malware Protection
- Intrusion Detection
- Physical Protection
- Centralized Logging

Departmental Standards

- Goes further than university policies and addresses issues specific to our department
  - Conflict of Interest
  - Computer Administrator Access Standard
  - Student Computer Access Standard
  - Work Standard

CIS Benchmarks

- CIS Benchmarks
  - Turn off unnecessary settings to protect systems
  - We have used their system benchmarks for 15+ years
  - The benchmarks can take significant amounts of time to implement
  - Often the benchmark will break a break 3rd party software packages
  - The benchmarks have kept us from major purchases of 3rd party apps.

Tools and Solutions

- Cloud Endpoint Management
- Cloud Endpoint Protection
- Cloud Storage
- Cloud Backup
- Cloud Password Managers

Cloud Endpoint Management

- Significant economies of scale with number of devices supported
- Critical in a Zero-Tolerence network model
- Critical in a remote/hybrid workforce model
- Examples
  - Useful to find misplaced/stolen/lost equipment.
  - Extremely useful during Covid

Cloud Endpoint Protection

- Fills a current gap in our current cyber-security defense
- Tool to assist protection in a remote workforce
- Cloud based
- Automatic investigation and remediation
- Unified security management
- Protect user identities and reduce the attack surface
- Identifies anomalies with adaptive built-in intelligence, giving you insights into suspicious activities and events, revealing the advanced threats, compromised users, and insider threats facing your organization.
- Sensors monitor and provide a comprehensive view for all user activities from every device.

Passwords and Password Managers

- According to Verizon's 2017 Data Breach Investigation report, 81% of data breaches are caused by poor credential management
- BAMS used to maintain notebooks with handwritten passwords locked up in a safe
  - It worked but there were always issues with poor handwriting and finding the password in the book started to become unmanageable.
  - Roughly 4 years ago, a password manager was finally approved by the University
- Password managers allow generation of secure passwords, so you are not reusing passwords
- Checks your passwords for reuse

Ransomware

- Ransomware has been around for years
- Cryptocurrencies has made it more prevalent, since it is more difficult to trace
- Global ransomware damage costs to reach $20 billion by 2021
- In the news this past weekend, with an attack on a gas pipeline (Colonial Pipeline)
- Backups are an effective means to recover from an attack

Spear Phishing

- Gift card scam has been an issue for the last few years
- We registered our VIPs in advanced threat protection
- Any email sent impersonating them gets flagged in the email
- The issue, all users have to be registered with this module, so there is a licensing fee

IoT

- Printers
- Conference Room Equipment
- Security Cameras
- Smart speakers

Covid

- In a sort period, we moved most staff to remote
  - 2 points in my career have been life changing, drop everything and go into crises mode (April 16th and Covid)
  - Not enough licenses for VPN
  - Increased phishing attempts

- FBI reported up to 4,000 new cybersecurity complaints per day 400% increase, after the onset of the pandemic.

Post Covid

- Increased efficiency may be attributed to not commuting, minimized workplace distractions and more freedom to work during the hours that are best for everyone.
- Invest in next generation tools to help manage users and data
- Implement new strategies is critical to securing remote employees, protecting their digital assets and guarding against cyberthreats.
- The Covid-19 pandemic triggered an accelerated migration of business applications and infrastructure into the cloud.
- 76% of companies adopted cloud services faster than they had planned, which unintentionally increased attack surfaces and created security gaps for hackers.

Managing Cybersecurity In The Hybrid Workplace

- Companies to consider a long-term plan on how to provide security to employees and protect their digital assets at a time when cybercriminals have a bigger attack surface to target.
- The time has come for a more strategic approach to security as companies settle into new hybrid workforces that support remote work.
- Covid-19 has challenged and changed how many of us do our jobs, yet with good direction, thoughtful strategies and the right technology, working remotely in a hybrid workplace can be a change for the good in the post-pandemic world.