Managing Cybersecurity Concerns Under Budgetary Constraints

Thomas L. Tyler Jr., Cybersecurity Advisor
11.12.20

CAPINTECH

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.


COR NAVIRUS
[COVID-19]
VACCINE RESEARCH 0034 - 234


Closed due to
CORONAVIRUS


GET ME OUT OF HERE

March 2020

- "Unprecedented Shift"
  - Over 60% of Americans are working from home during the crisis
- Companies have extended WFH orders through 2020
- 74% of CEOs expect some permanent shift

Zillow VISA

Attempting to Work

- Non-traditional work environment
  - Lack of structured schedule
  - Traditional management techniques
- Remote access onboarding
  - New devices or BYOD
  - Rural Internet issues

Attempting to Work

- Cross-training roles
  - Managing segregation of duties
- Added security requirements
  - No longer one network to protect
  - Security layers translate to home network

Flexibility But Within Boundaries

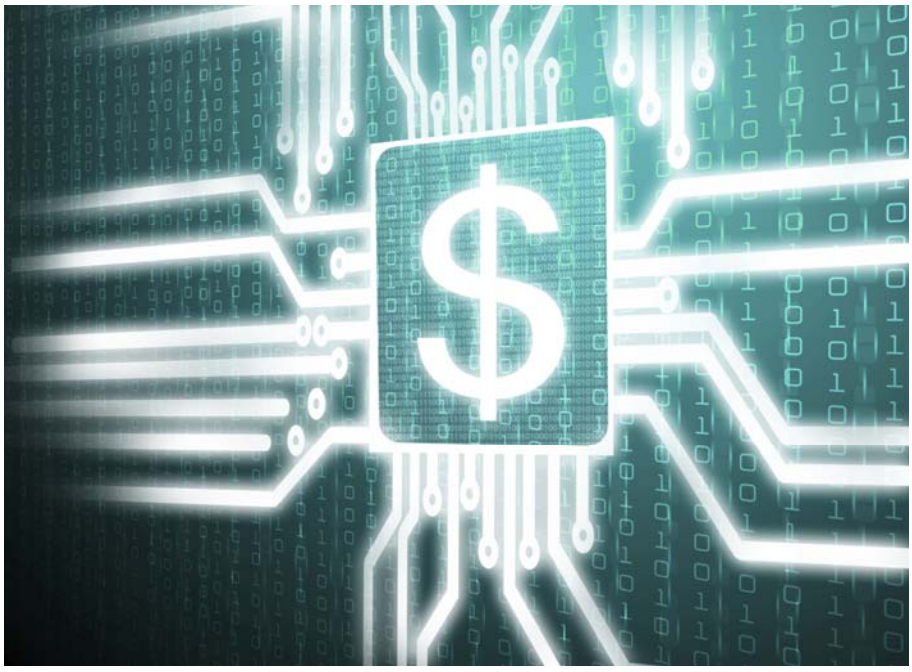
- Technology, processes, and culture should be considered
- Should include everyone: executive management to entry-level employees
- Practical and moral support should be provided to ensure success for onsite and WFH employees

All-Inclusive Collaboration

- Employees need tools to be effective
- Understand your existing products and services
  - Ineffective tools and applications hinder performance
  - Adds frustration and stress
- Consider your audience – employee vs. constituent

All-Inclusive Collaboration

- Communication becomes key
  - More than necessary, but becomes second nature
  - Numerous methods
  - Ends up being less intrusive
- Isolation becomes a valid issue
  - Lack of casual interchanges




DAILY
World • Eco
ght © Daily News XXII
Cyber attack
orld's leaders meet to-
day to discuss global
nd terrorism is

Security Concerns

- Third-party vendors
- Organization responsibilities
- End-user assistance

Third-Party Vendors

- New vendors
  - Risk assessment
  - Contract review
  - Approval procedures
- Existing vendor relationships
  - Periodic oversight procedures
  - Utilizing existing resources

Emergency Vendor Considerations

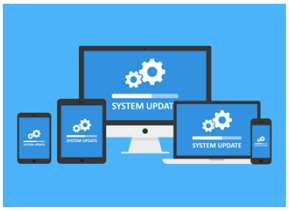
- Pull and review System and Organization Controls (SOC) reports
- Review any contracts
- Research what others have implemented
  - Hardening controls
  - Proper implementation procedures
  - Possible mistakes

Existing Vendor Resources

- Use existing vendor relationships
  - Managed service providers
  - Accounting platforms
  - Donor management, CRMs, etc.

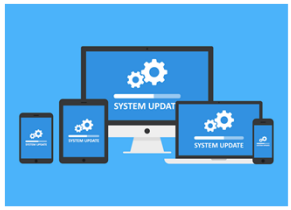
Device Management

- Centralized system
  - All devices receive latest updates or definition files
  - Remediate issues
- Manual process
- Limit access
  - Application and browser add-ons
  - Avoid sharing devices



Device Management

- Personal Devices
  - Update and secure across home network
    - Patch and anti-malware management
  - Router, streaming devices, voice assistants, appliances, smart home devices
  - Obsolete software



Mobile Devices

- Inherent threats for devices
- Establish Acceptable Use Policy (AUP)
- Maintain inventory, regardless of ownership
- Enforce restrictions
  - Passwords/biometrics
  - Encryption
  - Remote wipe

Mobile Devices

- Consider mobile device management (MDM) software
- Establish data removal procedures
- Cloud data restrictions

IoT Devices

- Inventory devices in use
- Layered security controls
  - Strong passwords
  - Evaluate data and analytics sharing
  - Patching procedures
  - Disable features
  - Segmented network

Password Security

- Numbers, characters, symbols
- Avoid common words
- Change often, and when compromised
- # of characters (8…12…??)

Password Security

- 7 characters – 0.29 milliseconds
- 8 characters – 5 hours
- 9 characters – 5 days
- 10 characters – 4 months
- 11 characters – 1 decade
- 12 characters – 2 centuries

Password Security

- Unique and private passwords
  - Password manager?
- Business ≠ Personal
- Account lockout and inactivity threshold
- Biometrics
- Layered security

Multi-Factor Authentication

- Critical for all cloud applications
  - Remote access
  - Email
  - AWS/Azure
- Consider IP address, time, and day restrictions
- Mobile devices, email message, tokens

Encryption

- All connections should be protected
- Data sent and received
  - In transit
  - At rest

User Provisioning and Access

- Minimum rights for users
- Review regularly
  - Job transfers
  - No longer needed

Wi-Fi Networks

- Use properly secured Wi-Fi
  - Work and home
  - Be wary of public Wi-Fi
  - Use a VPN
  - Mobile hotspots

Wi-Fi Networks

- Encrypt network appropriately (at least WPA2)
- Secure password for access
- Guest network for non-business system

Limit Application Programming Interface (API)

- Allows applications to communicate with each other
- Enhances functionality of cloud apps
- Bridges internal network resources with cloud apps
- Can introduce new risks due to elevated privilege of APIs

Consider Data Loss Prevention (DLP)

- Preventing end users from sharing critical data outside of the intended use
  - Downloading data from the cloud
  - Using cloud apps to share critical data

Data Retention Periods

- Large amounts of data may be stored
- Limit impact if data or systems are compromised
- Evaluate and establish removal process

Shadow IT

- Apps or devices that are utilized without IT knowledge
  - Personal or mobile devices
- Rogue cloud services
  - Personal email, document scanning, cloud storage
- Appropriate authorization procedures

Training

- All employees should participate
- Methods will vary — webinar, email, newsletters, etc.
- Review policies and procedures
- Real-world examples
- Build culture of awareness
- Establish Incident Response Plan

Key Takeaways

- New threats to consider that weren't on our radar 12 months ago
- Loss of reputation can be significant
- Maintain adequate security controls
  - Provide critical tools for users
  - Doesn't have to be expensive!

Thanks!

Thomas L. Tyler Jr.
Cybersecurity Advisor

ttyler@capincrouse.com
505.50.CAPIN ext. 2009

CAPINTECH