KMK | Law

Ascend TECHNOLOGIES

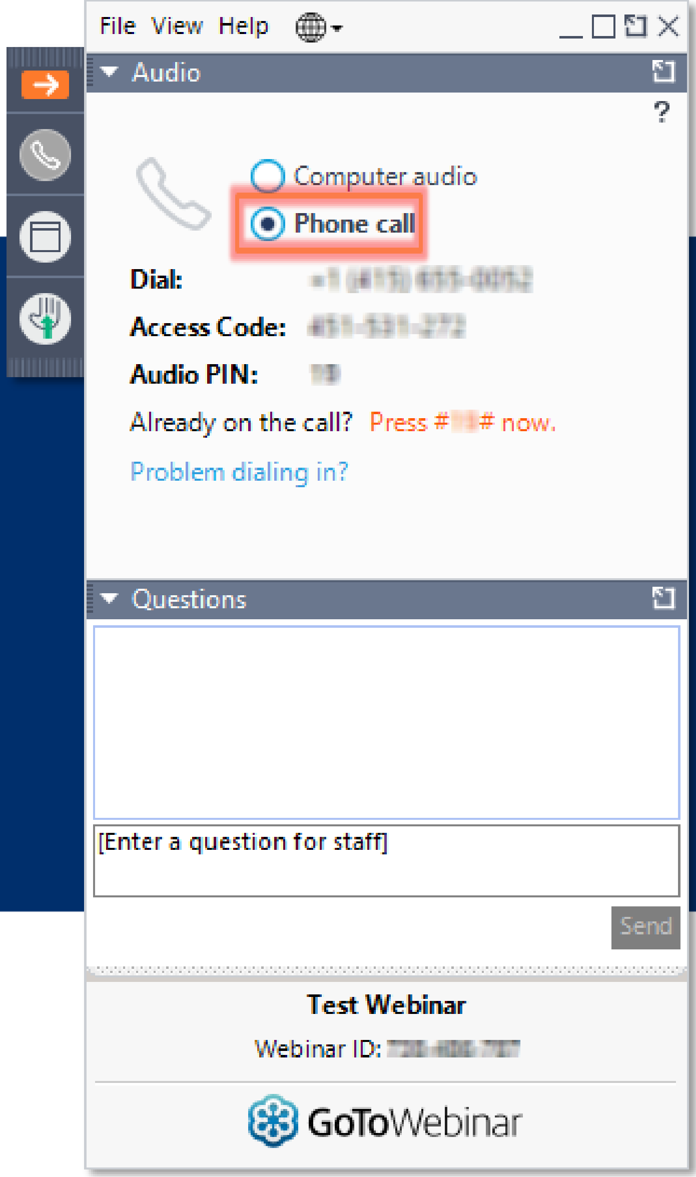
Data Protection & Cybersecurity in a Remote-Work Environment

WEBINAR:

Friday,
April 24, 2020

KMK | Law

- Select “Computer audio” to join via VOIP
- Select “Phone call” to dial in



○ Computer audio
● Phone call

Dial: [redacted]
Access Code: [redacted]
Audio PIN: [redacted]
Already on the call? Press #[redacted]# now.
Problem dialing in?

[Enter a question for staff]

Test Webinar
Webinar ID: [redacted]

GoToWebinar

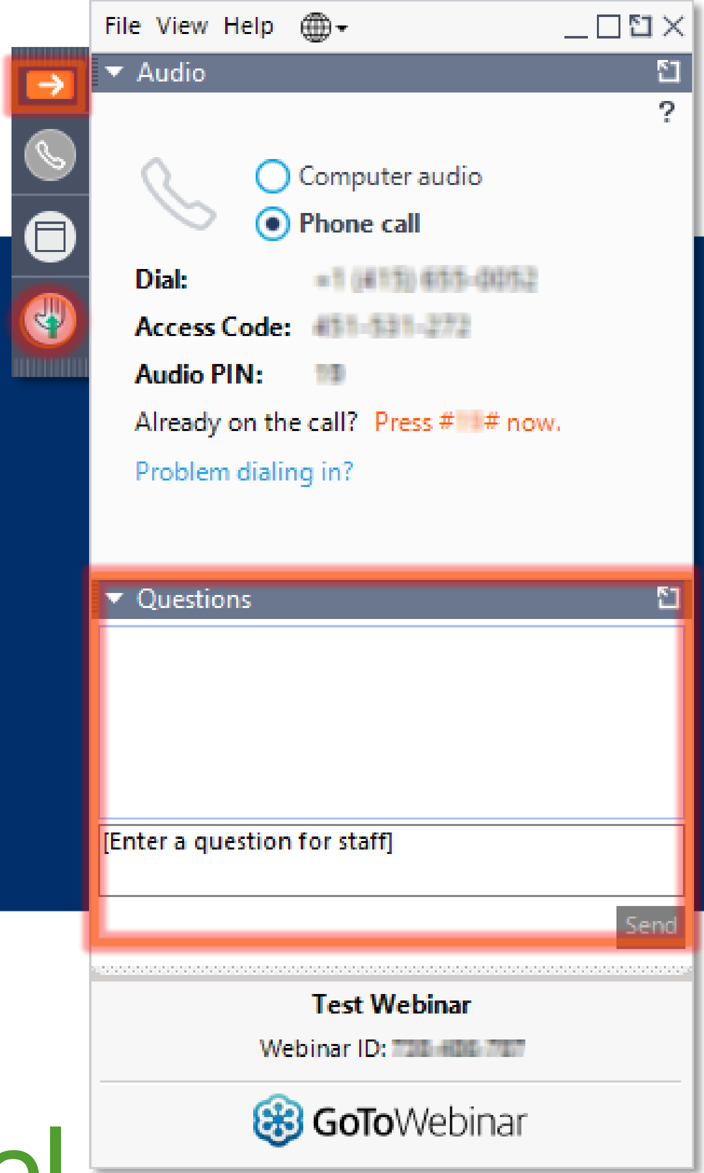
Ascend TECHNOLOGIES

Audio Instructions

KMK | Law

- Grab Tab
- Handouts
- Questions

Attendee Control Panel



○ Computer audio
● Phone call

Dial: [redacted]
Access Code: [redacted]
Audio PIN: [redacted]

Already on the call? Press #[redacted]# now.

Problem dialing in?

[Enter a question for staff]

Test Webinar
Webinar ID: [redacted]

Ascend TECHNOLOGIES

Objectives

- Update on recent ransomware events and cyber activity
- Challenges associated with video conferencing and other services
- 10 Reminders of best practices for data protection in a remote-work environment

KMK | Law

Meet the Speakers

Joe Callow
Partner
KMK Law
513.579.6419
jcallow@kmklaw.com

Drew Hicks
Partner
KMKLaw
513.579.6565
dhicks@kmklaw.com

Stephanie Scott
Associate
KMK Law
513.579.6582
sscott@kmklaw.com

Rich Wills
Chief Information Officer
KMK Law
513.579.6588
rwills@kmklaw.com

Mike Manske
VP, Cybersecurity
Ascend Technologies
312.980.9431
mmanske@teamascend.com

Justin Maynard
VP, Solutions Architecture
Ascend Technologies
312.980.9980
jmaynard@teamascend.com

Ascend
TECHNOLOGIES

KMK | Law

Update on recent ransomware events and cyber activity

Ascend TECHNOLOGIES

Recent Security Headlines

Credential phishing emails have been the most commonly observed threat that has incorporated COVID-19

FBI Warns of Teleconferencing and Online Classroom Hijacking During COVID-19 Pandemic

Cognizant Hit by 'Maze' Ransomware Attack

April 2020

Cyber insurer Chubb had data stolen in Maze ransomware attack

March 2020

Ryuk Ransomware operators continue to target hospitals during COVID-19 outbreak

Changing Threat Landscape with Remote Workforce

1) Phishing and Ransomware

- **148% increase** in ransomware emails,
- Emails posing as information on Coronavirus
- More impactful with people remote… IT can’t respond in the ways they have in the past

Changing Threat Landscape with Remote Workforce

2) Remote Access and Data Exposure

- Employees using **unmonitored and unsecured networks**
- Data loss through employees **taking information home** and using personal devices (e.g. Dropbox)
- “Shadow IT” for remote access and collaboration tools
- Security team cannot perform necessary operational activities

Changing Threat Landscape with Remote Workforce

3) Security Incident Response

- Security incidents have increased… **Can your company respond if everyone is remote**?
- Shutting down remote capabilities may not be an option.
- Most of the normal action taken in the past would ruin productivity

Phishing Scams

How have consumer scams change?

- Companies advertising remedies and treatment of COVID-19
- Fake charities or hospitals requesting donations
- Fraudulent calls and text messages impersonating banks with COVID-19 relief checks

Top Recommendations

- Educated employees
- Conduct mock phishing training campaigns
- Enhance email security controls

Additional Recommendations

- Reset passwords for users who have visited suspicions Coronavirus domains
- Customize login pages (i.e. don’t use the default O365 login page)

93% Breaches include phishing

Malware and Ransomware

How has Ransomware evolved?

- Significant increase in phishing emails
- Increased volume of MFA enrollment requests from unusual locations

Top Recommendations

- When possible, enabled multifactor authentication (MFA)
- Restrict user's ability (permissions) to install and run unwanted software applications
- Deploy next generation antivirus tool

Additional Recommendations

- Regularly apply system and software updates
- Enable strong passwords and account lockout policies to defend against brute force attacks.
- Maintain a good back-up strategy
- Apply the practice of least privilege
- Scan for and remove suspicious email attachment
- Ensure that only required users have administrator privileges
- Apply conditional access policies
- Disable macros in Microsoft Office applications

34% businesses hit with malware took **a week** or more to regain access to their data

Remote Access and Data Exposure

How is remote access riskier than before COVID-19?

- Inadvertent remote access vulnerabilities
- IT is unable to manage remote devices (i.e. patch, apply policies)
- Data loss through unapproved collaboration tools

Top Recommendations

- Audit public facing systems
- Backup remote access systems and configurations
- Use mobile device management (MDM) to maintain consistent security standard

Additional Recommendations

- Document and communicate BYOD policy to employees
- Educate employees not to remove confidential or sensitive information from your network (e.g., person email, USB drives, etc)
- Ensure that remote access mechanisms require MFA
- Maintain security configurations standards and continue to apply updates and patch remote devices

The exposure of Remote Desktop Protocol has grown **18%** between March 6th and 24th

Security Incident Response

How do we respond to security incidents with a remote workforce?

- Can you respond if everyone is remote?
- Shutting down remote capabilities may not be an option

Top Recommendations

- Conduct exercises to simulate an incident where multiple members of response team are unavailable or working remotely
- Ensure anti-virus tools leveraging endpoint detection and response (EDR) are installed on all endpoints

Additional Recommendations

- Review and update incident response plans to ensure security incidents can be addressed and responded to with a remote workforce
- Is contact information correct? Are cell phone numbers listed?
- Does your team have a physical copy of the plan?
- Communicate to employees on who they should contract in they have been a victim of a security incident

15 HOURS OR LESS The amount of time it takes majority of hackers to breach and exfiltrate data

Challenges associated with video conferencing and other services

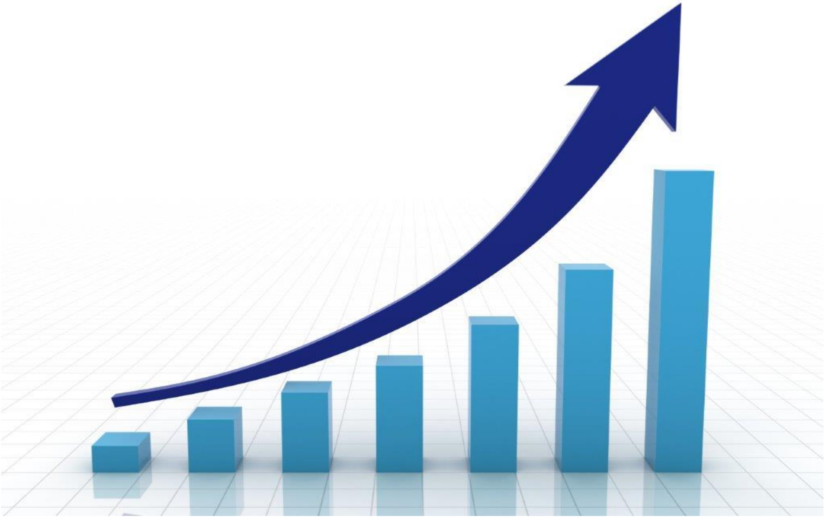
Popularity of Zoom and Other Video Conferencing Applications

- As employees continue to work from home, more and more businesses (including courts) are turning to alternative forms of face-to-face meetings

- Companies and individuals are increasingly utilizing video conferencing applications to facilitate meetings

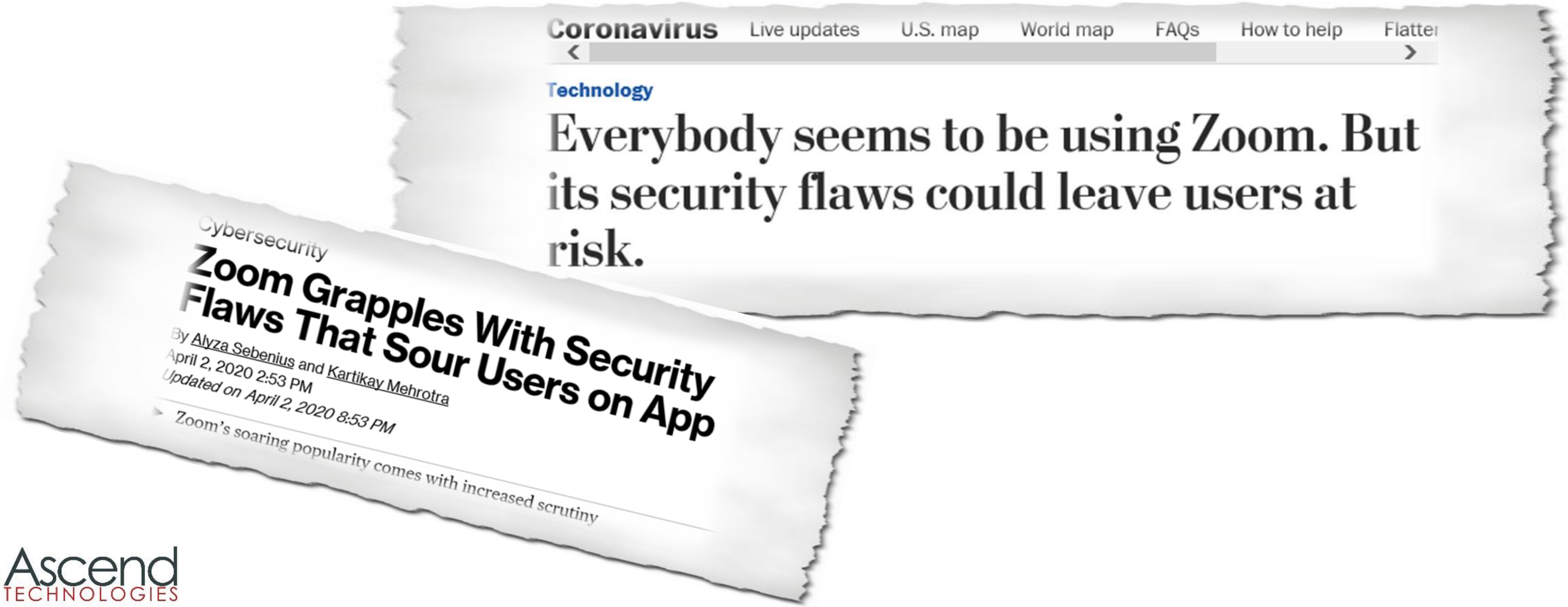
Popularity of Zoom and Other Video Conferencing Applications

- For example, Zoom → popular form of video chat, has nearly 200 million user-meetings daily
- Increase of 2000% since December of last year



The Dark Side of Zoom and Other Video Conferencing Applications

- With increase in popularity, Zoom has seen spike in security threats



Technology

Everybody seems to be using Zoom. But its security flaws could leave users at risk.

Cybersecurity

Zoom Grapples With Security Flaws That Sour Users on App

By Alyza Sebenius and Kartikay Mehrotra
April 2, 2020 2:53 PM
Updated on April 2, 2020 8:53 PM

Zoom's soaring popularity comes with increased scrutiny

The Dark Side of Zoom and Other Video Conferencing Applications

- Zoom has issued multiple statements relating to increase in security threats in the face of several consumer complaints and class-action lawsuits

> *" However, we did not design the product with the foresight that, in a matter of weeks, every person in the world would suddenly be working, studying, and socializing from home. We now have a much broader set of users who are utilizing our product ina myriad of unexpected ways, presenting us with challenges we did not anticipate when the platform was conceived."*
>
> *- Eric S. Yuan, Founder and CEO, Zoom*
>
> zoomblog
> April 1, 2020
> "A Message to Our Users"

Tips to Stay Safe While Using Zoom and Other Video Conferencing Applications

- Users should be aware and become familiar with the privacy settings available within the video conferencing application and set all meetings to “private”

- Users should not use a generic Personal ID meeting code for meetings, and instead create a unique code per-meeting
  - In addition, users should be careful of how they are sharing their meeting “links” (hyperlinks which allow other users to access the virtual meetings directly) and not share the links publically or post them on social media

Tips to Stay Safe While Using Zoom and Other Video Conferencing Applications

- Meeting hosts should also utilize the “waiting room” function, which allows them to see who is trying to join the meeting and gives the option to grant or deny a user access before joining

- Once the meeting has begun and all users are present, hosts should utilize the option to “lock down” the meeting, preventing any new users from joining

Tips to Stay Safe While Using Zoom and Other Video Conferencing Applications

- Whenever possible, device cameras should be covered when not in use

Tips to Stay Safe While Using Zoom and Other Video Conferencing Applications

- Users should continue to be aware and on high-alert for new security threats and continue to take steps to protect themselves and their organizations

- Make sure using the application does not run afoul of cybersecurity policies

- Important that security threat risks do not outweigh the benefits of using applications

KMK | Law

10 Reminders of Best Practices For Data Protection In Remote-Work Environment

Ascend TECHNOLOGIES

10 Reminders For Data Protection In Remote-Work Environment

1) Change Passwords

- Complex
- Set Expiration
- Two Factor Authentication

10 Reminders For Data Protection In Remote-Work Environment

2) Limit/Control Access to Data

- Evaluate operations
- Consider segmenting your network
- Consider temporarily limiting access to certain data

10 Reminders For Data Protection In Remote-Work Environment

3) Deactivate Unused or Noncritical Data

- Evaluate what data is needed and what is not
- Deactivate data not currently needed or not being used

10 Reminders For Data Protection In Remote-Work Environment

4) Make Backups and Store Offline

- Ensure backups are stored on a network segment not accessible to rest of your data
- Store copy of each backup offsite
- Verify backups are working and data can be restored

10 Reminders For Data Protection In Remote-Work Environment

5) Remind Employees About Their Training

- Simple Mistakes = Data Breach
- Reinforce training and remind employees about malicious phishing emails
- Employees are greatest threat and greatest asset
- If you don’t have training, now is good time to start

10 Reminders For Data Protection In Remote-Work Environment

6) Encrypt Sensitive Information

- Working at home invites informality
- Make sure encryption policies are followed

10 Reminders For Data Protection In Remote-Work Environment

7) Check Firewalls and Confirm Security

- Evaluate effectiveness of firewalls and security measures
- Patch all systems and keep security up-to-date

10 Reminders For Data Protection In Remote-Work Environment

8) Confirm Process In Place to Deal With Data Breach

- Incident Response Plan?
- Need Written Plan

Plan Considerations

- Legal Counsel
- Insurance Carrier
- Verify Breach
- Contain and Mitigate Breach
- Preserve Evidence/Log
- Communications Protocol

Guidance/Reference

- National Institute of Standards and Technology (NIST)
- Federal Trade Commission
- Securities & Exchange Commission
- Department of Homeland Security
- Chamber of Commerce

10 Reminders For Data Protection In Remote-Work Environment

9) Install Security Patches On Remote Computers

- Ask all work-from-home employees to apply security patches/updates to home computers
- Significantly reduce security threat

10 Reminders For Data Protection In Remote-Work Environment

10) Keep Up On Current Events

- Cyber landscape changes regularly
- Learn and adapt

Helpful Resources

- FTC: Protecting Small Businesses (https://www.ftc.gov/tips-advice/business-center/small-businesses)

- FTC's Start with Security: A Guide for Business (https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business).

  (1) Start with security
  (2) Control access to data sensibly
  (3) Require secure passwords and authentication
  (4) Store sensitive personal information securely and protect it during transmission
  (5) Segment your network and monitor who's trying to get in and out
  (6) Secure remote access to your network
  (7) Apply sound security practices when developing new products
  (8) Make sure your service providers implement reasonable security measures
  (9) Put procedures in place to keep your security current and address vulnerabilities that may arise
  (10) Secure paper, physical media, and devices.

Helpful Resources

- SEC Commission Statement and Guidance on Public Company Cybersecurity Disclosures, 83 Fed. Reg. 8,166 (Feb. 26, 2018).
- FCC Cybersecurity for Small Business (https://www.fcc.gov/general/cybersecurity-small-business).
- US Chamber of Commerce: Internet Security Essentials for Business 2.0 (https://www.uschamber.com/sites/default/files/legacy/issues/defense/files/020956_PDF_web.pdf).

Helpful Resources

- April 2018: Cybersecurity Framework 1.1 (https://www.nist.gov/cyberframework).

- Sept. 9, 2019: NIST Requests Comments on Draft Privacy Framework (https://www.nist.gov/news-events/news/2019/09/nist-requests-comments-draft-privacy-framework).

KMK | Law

We provide effective data protection and cybersecurity solutions to minimize risk before, during, and after a data breach.

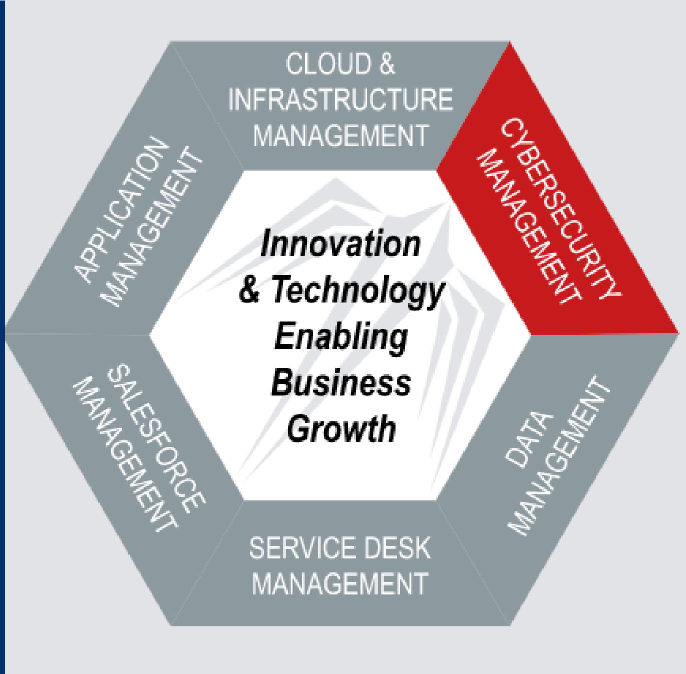
To learn more about KMK's Cybersecurity & Privacy Team visit **www.kmklaw.com**

Ascend TECHNOLOGIES

KMK | Law

We provide comprehensive security services designed to protect your institution from cyber threats that are growing in both frequency and sophistication.

For more information, please visit **www.teamascend.com**



Ascend TECHNOLOGIES

Contact Us

Joe Callow
Partner
KMK Law
513.579.6419
jcallow@kmklaw.com

Drew Hicks
Partner
KMKLaw
513.579.6565
dhicks@kmklaw.com

Stephanie Scott
Associate
KMK Law
513.579.6582
sscott@kmklaw.com

Rich Wills
Chief Information Officer
KMK Law
513.579.6588
rwills@kmklaw.com

Mike Manske
VP, Cybersecurity
Ascend Technologies
312.980.9431
mmanske@teamascend.com

Justin Maynard
VP, Solutions Architecture
Ascend Technologies
312.980.9980
jmaynard@teamascend.com