KNOWLEDGE MANAGEMENT AND THE NEW NORMAL

April 30,2020 • KM World • Joyce Wells

With the rise of the COVID-19 crisis, regular business practices were upended with little warning. Video conferencing and collaboration platforms enable workforce interaction and customer contact to continue despite nearly ubiquitous work-from-home schedules. However, some organizations are also beginning to recognize the security and privacy risks associated with these out-of-office scenarios and, as a result, are seeking to ensure that they have the right tools in place to mitigate any weaknesses.

Recently, James Carroll, partner and director at TetraVX, a unified communications and collaboration company that specializes in the delivery of cloud-based solutions, and Kevin Beasley, CIO at VAI, an ERP software developer, discussed what should and should not be shared using collaboration tools, platform design features to look for, the security issues involved, and how to protect sensitive documents at risk of exposure.

KMWorld:
We are in a unique time with social distancing protocols and new work from home rules. For companies that have had employees working remotely before as well as organizations that are new to work from home best practices, what should they be thinking about now as far as privacy and security?

Kevin Beasley:
Because organizations were required to quickly transition to a fully-remote workforce, many companies were ill-prepared for the security and privacy issues associated with working from home. Even if the organization already had a work-from-home policy in place, the difference between a few remote workers accessing systems and dozens to thousands of employees is substantial in terms of security and scalability.

Malware attacks could increase now that employees are using less secure networks or video conferencing tools that aren't a part of their organization's security framework. It's crucial for companies to accelerate their security and privacy mandates and implement stronger protections for their IT system. This also includes protecting the privacy of employees and securing business applications from any bad actors or unauthorized access.

James Carroll:
Privacy and security are always a challenge, but that challenge heightens when you think about the additional complications of working from home. Personal device use, home networks, unlocked laptops, and more can lead to additional security issues that may have been limited in an office. To ensure your employees are staying secure while at home, it's important to focus on both training and technology. Solutions that offer desktops as a service can help provide a secure access

point for users but it's just as important to make sure the users are trained on how to use it and what security concerns to look out for and avoid.

KMW: What should and should not be shared over collaboration tools?

JC: Knowing what information to share across collaboration tools comes from both situational requirements and data sensitivity. Is this a document that holds the personal addresses of employees? That type of document would not require collaboration and holds sensitive personal information, and therefore shouldn't be stored or shared in your collaboration platform. Is it a sales presentation that needs multiple contributors and doesn't hold sensitive information? That would be a perfect fit. It's important to have strong collaboration governance in place and train your users on the best practices of engaging with one another and with their clients using these platforms.

KMW: What are the design features to look for and use?

JC: Security tools like advanced threat protection [ATP], OAuth for access delegation, Transport Layer Security [TLS], Secure Real-Time Transport Protocol [SRTP], and other industry-standard encryption techniques can all be used to limit the security risks your organization is susceptible to. It's important to make sure your provider has considered security in its earliest stages of development.

KMW: What should be considered in terms of protecting sensitive documents at risk of exposure when shared over a collaboration platform?

JC: Securing sensitive documents via password protection or private collaboration groups should be step one in creating barriers between which documents can be accessed by the larger organization.

KMW: What are the top security threats organizations should be aware of?

KB: Beyond the common security threats that today's businesses face, organizations must look out for additional threats and suspicious activities that are heightened for remote work. Malware and phishing attacks can be difficult to track without employees taking IT assets home while logging in from new networks, so security teams must be installing additional multi-factor authentication for logins and policies to protect user passwords and access.

This also includes access from mobile devices associated with employee email accounts or mobile logins for business applications. Insecure interfaces and APIs also present a major risk that can expose organizations to breaches and bad actors. To protect against these risks, virtual private networks must have additional security mandates and automated alerts in place.

KMW: Are there technological architectural considerations that organizations need to have in mind to combat these issues?

KB: There are a few considerations organizations need to have built into their architecture to protect their network. It's important to have a security-first environment by installing additional layers of security infrastructure between the operating system and hardware platform. This includes having continuous security testing and automating scans of hardware and software systems to seek out vulnerabilities and patch potential issues as they arise. While many of these security issues were common before people worked from home, the most critical point to consider with regard to remote

work is the architecture of your network. Maintaining security and access control and a layer of detection to the network is critical to protect against the most complicated malware attacks.

KMW: Does cloud computing cut down on or increase security risks?

KB: While there has sometimes been a perception that the cloud is less secure than on-premise infrastructure, it's actually the opposite in most cases. A private cloud environment and some public clouds offers an increased layer of protection and risk mitigation by employing a security-first approach with automated checks and layers to the system. In partnership with the service provider, companies who implement security monitoring and access controls can ensure access to applications hosted in the cloud remain secure. The flexibility of the cloud makes it more functional to connect various networks together and layer in security throughout, rather than having separate systems that are difficult to maintain and track on one centralized platform. In addition, new and safer technologies such as replacing System Message Block protocol and mapped drive letters with secure file transfers such as HTTPS, FTPS, or WebDAV [Web Distributed Authoring and Versioning] for internet-based file storage can help protect companies from ransomware attacks.

KMW: When this is over, what should companies learn from this experience so they can improve their practices in the unfortunate event something like this happens again?

KB: Companies will learn a lot from this experience that will force them to put an increased focus on security and business continuity planning moving forward. While no one predicted the scale of this, organizations should always be preparing for crises and ensure they have secure systems and BCP and disaster recovery capability in place to handle a large disruption to business.

Another major lesson we see coming out of this is that many companies will implement more flexible work from home policies now that they have learned how to secure and scale remote environments. The ability to enable remote work is extremely beneficial during crisis events, and we see many businesses making sure they're able to securely allow their employees to work from home from now on.

JC: The reality is that working from home won't go away and that security will always be a concern. It's important to include your work from home security strategy as an ongoing priority even after COVID-19 is behind us.