Unified Communications in Higher Education

Responding to New Risks

ECAR

ECAR Working Group Paper | November 17, 2015

ECAR working groups are where EDUCAUSE members come together to create solutions to today's problems and provide insight into higher education IT's tomorrow. Individuals at EDUCAUSE member institutions are invited to collaborate on projects that address core technology challenges and advance emerging technologies important to colleges and universities. More information can be found at the ECAR working groups website.

Introduction: Everyone Is Connected

New unified communications (UC) capabilities and the increased desire for richer collaboration experiences have led to a fundamental shift in the technology we use for communication.[1] For many decades we have worked with and managed risks in a world where traditional telephone service was the primary method for voice communication. But in a UC world, the risks change. What assumptions are different in this environment about how people communicate, and what must IT do differently to assess and plan for the risks in this space?

Moving into UC includes some necessary risk. Understanding what the risks are, knowing who is responsible for them, and planning for them will help ensure a successful transition. This paper discusses issues such as survivability, privacy, discoverability, and emergency communications in a converged-communications environment. It is meant to inform both implementers and those who make risk-assessment decisions—including CIOs, senior IT leaders, and campus communications technology planners and implementers—about risks in the modern age of communications in the light of a change from a traditional phone system to broader/unified communications platforms. The paper is also meant to spur conversations with campus partners such as risk management, safety, and compliance officers—the people who ultimately assess and even make decisions based on risk and on the local, state, and federal regulations to which they are subject. In addition, it is intended to inform and bridge discussions with industry representatives who are necessary partners in this arena.

The paper looks at four key areas where risk plays a strong part in modern-day communications:

- Survivability of the communications infrastructure
- Communications during emergencies
- Data privacy, security, and compliance
- Data storage

Each of these includes an explanation of the topic, an identification of current trends, and a discussion of the risks and ways to mitigate them. As opposed to prescribing specific actions, the paper aims to inform

EDUCAUSE

readers of the emerging state of the domain in the light of the change from a traditional phone system to a broader UC platform.

Survivability of the Communications Infrastructure

For many decades, wired telephone systems were the single essential tool that people used to communicate for business and summon help. There were simply no other options available to most people. This reliance—on a single mechanism for communication and for access to assistance in emergency situations—resulted in telephone systems' being designed for extreme reliability. This included fully fault-tolerant central switching designs, simple end-user instruments, and backup power that kept telephones working even when most other infrastructure in an area was damaged by a natural disaster or other event. High reliability comes at a high cost, though, both in terms of building and operating the service and—because of the rigid designs—of offering few options for flexible features that end users desire. In recent times most people are connected in multiple ways, with office phones, cellular phones, home phones (or not), and a proliferation of alternative communication such as instant messaging, e-mail, Facebook, Twitter, and other examples of social media. Many of these newer forms of communication are also able to summon emergency assistance and are preferred for such usage by a growing portion of the user base. The traditional landline telephone is a less important communication tool for most people.

In a world where everyone is multiply connected, what is the optimal set of investments that we should be making to enhance the communications environment while still providing for access in times of emergency? The key network infrastructure components that support our modern communications environment include:

- **Wired Data Network:** This network provides data network services, network connectivity, and electricity to wireless network access points and often powers desktop telephones. Building control, alarm, and security systems may be carried by the building's data network. Most of these services stop when the network goes down, whether the reason was scheduled or unscheduled. Service outages due to network switch and server maintenance cycles may be unfamiliar to legacy voice users. Some critical services (e.g., fire alarms) may have a private backup communications solution.
- **Carrier Cellular Network:** The cellular carriers operate parallel wireless networks that provide general voice and lower-speed data services directly to end-user devices located at our facilities. While these carrier networks are often challenged to work well within buildings, they generally provide acceptable performance, especially for voice calls, when outdoors.
- **Cellular Distributed Antenna Systems (DAS) Network:** DAS solutions generally provide strong and reliable cellular coverage, both in terms of signal strength and enhanced network capacity, within buildings.[2] DAS solutions are more likely to depend on building power and independent backup resources.

We define *communications survivability* in the multiply connected world as a high probability that an individual will be able to communicate as needed, via some mechanism, for business continuity and emergency communications. Each of the network types described above provides a form of communication to the end user and has different characteristics and different cost points for maintaining operations during emergency situations, typically when the power is out. A risk-based approach to investment decisions for redundant power, cooling, and electronics for each of these networks can lead to significant savings while still providing the services needed by the end users.

One relatively new factor that should be considered as part of your overall network-durability investment decision process is connectivity for endpoint equipment that is used to control physical devices (i.e., supervisory control and data-acquisition systems) such as air conditioning, freezers, and pumps. These devices are increasingly connected to the main campus network and might not be configured with independent backup communications. How long can these control systems continue to do their job in an offline mode? Is independent backup connectivity, when needed, a more effective strategy than financing increased main-network durability?

Emerging Trends

Some stakeholders—such as campus security staff, risk officers, and even end users—have the mind-set that telephony is life-safety equipment (in fact, this belief drives not only survivability but also power sources, which are discussed in the next section in more detail). However, trends in building codes and difficulties in duplicating legacy-level reliability in modern unified networks do not support this point of view.

The National Electric Code (NEC) (2008) §700.1 states, "Emergency systems are those systems legally required and classed as emergency by municipal, state or federal codes." NEC §700.6 (D) and §700.9 (B) describe the separation of emergency system circuits from all other circuits. International Building Code (IBC) (2009) §2702.2 lists the systems that are to be considered emergency loads. One should note that this section enumerates both emergency loads and standby loads. This section references the International Fire Code (IFC) (2009) §604 as well. A few more esoteric loads are included in the emergency systems by the IFC. Note that §604.2.15.2.1, which references emergency power loads for voice communication systems, refers only to underground buildings.

Telephony is not listed in either the IBC or the IFC as an emergency system. Therefore, under the Uniform Construction Code, they must not be intermingled with circuits supplying emergency systems. Essentially, this means that those wishing to converge services (e.g., VoIP, electronic access, video surveillance, wireless access points, etc.) onto a single edge network can do so—assuming that network does not support life-safety equipment—since there is no emergency power requirement for that infrastructure as a whole.

Increasingly there is an awareness that some level of survivability should be provided to the data network as a whole, at least in the interest of preventing device "flapping" (where the network status toggles between on and off) as the result of brownouts. But there is no specific survivability requirement, at least per code, for IP-based communication services, other than truly emergency-categorized systems (alarm panels, emergency phones, and so on). Overall, enterprises typically provide 5 to 15 minutes of UPS backup power. Generators are typically only provided in critical facilities, such as emergency services, health care, and so on. Some UC clients can be supported through a 911 partner, but even those solutions are limited to tightly constrained/controlled environments.

Risks and Mitigation

There is inherent risk in the increased complexity of a UC infrastructure. In a world where most students, staff, and faculty have multiple communication devices, including a mobile phone in their pocket, institutions need to think hard about where to invest for the survivability of UC. In an emergency, most will first reach for their mobile phones; in fact, it is estimated that "about 70 percent of 911 calls are placed from wireless phones, and that percentage is growing."[3] Therefore, providing emergency power to enterprise voice systems not only complicates and at times even prevents industry endeavors like LAN convergence, but it does so with minimal benefit.

Institutional priorities should fund those services that impact the largest set of users (e.g., redundancy and survivability in data center or central communication systems); that are key safety and security resources (e.g., elevator and other emergency phones); or that reinforce a strategic variety of systems in which to communicate (full survivability to all individual devices may not be financially feasible, but multiple devices using multiple platforms is already a reality).

Determining the standards for survivability (e.g., defining what is truly survivable) and educating the community about the institution's current/future-state environment compared to legacy communications will establish realistic expectations and result in better-informed communications choices.

Switches and Risk

Legacy telephone service is fairly simple to support. A voice switch has most of its critical components in one place, so there is only a single location to power and protect. That single switch also means that end-user devices receive power and connectivity from the one location over simple copper cabling.

UC, however, is delivered over a converged network that has many locations to power, protect, and possibly make redundant—and therefore has many potential points of failure. A converged network running on typical server architectures also introduces network-switch and server-maintenance cycles, translating to service interruptions that will be new to legacy voice users.

Communications during Emergencies

In the near past and throughout much of the history of electronic communication, the landline telephone was *the tool* used to summon emergency assistance. When an individual dialed 911, that call was carried over cable and electronics infrastructure dedicated to that one particular telephone line. Each of these hardline telephone circuits was highly reliable and terminated at a single address, enabling emergency dispatchers to provide the telephone's location to the appropriate emergency responders with each request for assistance. Being the primary and typically the only means to summon assistance, hard-wired telephone systems were designed and operated for extremely high reliability.

In today's environment individuals are multiply connected to several communications infrastructures in parallel. A typical office worker will have a desk phone, one or more handy computers, a cell phone and/or tablet, and nearby emergency devices such as an elevator or lobby phone. Any of these devices can be used to summon assistance. With the inherent diversity of the infrastructure that powers these devices, no single system needs to be operated at the level of reliability of the old hard-wired telephone system. Location transmission and the ability to even reach the right emergency center can be challenging with UC, and choices have to be made on how to deal with this (e.g., disabling 911 calls from UC entirely, or forcing users to click through a disclaimer that explains these challenges).

In addition, in a campus environment the assumption that the underlying networks that power the various devices are independent and effectively back each other up may not be accurate. For example, is indoor cellular coverage sufficient, or do individuals often need to go outdoors for their mobile devices to operate properly? Each campus needs to evaluate the interdependencies between the networks used to power user devices and ensure that the overall level of connectivity is appropriate during different times of emergency. Suggested evaluation factors include:

- **Electrical Power:** The single largest campus interdependency is likely to be electrical power. Building power is key to the operation of the wired and wireless data networks, and these networks underpin all UC services, e-mail, computer-based instant messaging services, and other similar communications infrastructure. The loss of building power typically causes the immediate loss of desktop computers and the delayed loss of laptop computers. Depending on the building's infrastructure, the wired and wireless data networks may survive for a short period of time on battery backup or may remain active permanently due to the presence of generator power. If a modern UC system is in place in the building, its devices typically shut down whenever the data network loses power. Buildings that leverage a distributed antenna system to ensure adequate cellular coverage typically have the same power reliability characteristics as the data network. The DAS either shuts down immediately when power is lost, survives for some period of time on battery backup, or remains online using generator-supplied power. Depending on the power infrastructure within a building and external cellular coverage, the loss of electrical power could cause a complete shutdown of all communications within a building. Evaluation factors for electrical power include:
    - ❖ Facility Requirements: Are individuals expected to leave the building during extended power outages, or do they need to remain for some specialized reason? If people are expected to exit the facility, your requirements for emergency power may be minimized but will still depend on regulations and the policies of your institution in general.
    - ❖ Data Network: The availability characteristics of a data network are proportional to the level of investment made in the network. A typical campus network will have a network core that uses redundant optical fiber connections and has generator-provided backup power to keep the core routers functioning during long power outages. Typically, no single fiber cut or power failure will disrupt the network core. By contrast, the investment made to keep the network to and within a building operational under various scenarios usually depends on business needs within the building. If people are supposed to leave the building during long power outages, the data network requires little added investment. On the other hand, a building that houses critical units such as the police department likely requires permanent full-network availability. Our general recommendation is that all buildings at least have UPS-supplied power that keeps the network operational long enough for people to cleanly shut down their work and leave the building, typically at least 30 minutes.
    - ❖ Cellular Service: Was a DAS installed to provide cellular coverage within the facility, or do sufficient outdoor cellular signals reach into the building to support emergency calling? If a DAS is needed for cellular coverage, how is it powered?
    - ❖ Last-Resort Communications**:** One campus strategy that has been growing in popularity as traditional telephones are replaced by UC platforms is the reuse of old interbuilding copper cable to provide a small volume of legacy analog telephone service. This service is hosted from the UC platform via analog gateways located in data centers with fully redundant power, cooling, and network connectivity. This type of analog service, while low in functionality, is highly reliable and can be used to provide service for a building's elevator, emergency, and courtesy phones. This service can survive extremely long power outages that extend even beyond what can be covered with local building generators. If this type of analog service is implemented, it can offset the need for generator power for the data network edge in many situations. These two tiers of voice service—high functionality/low reliability and low functionality/high reliability—are often the ends of a counterbalanced voice service continuum (if not the only two tiers) when moving to UC.
- **Endpoint Location:** The telephone and emergency-services community has invested heavily over the years in infrastructure to track the physical location of devices that call 911 so that location can be determined even if the callers are unsure of their street address. UC services, with their ability to provide connectivity anywhere there is a network connection, are often unable to provide accurate

location information. For example, a person traveling out of state dialing 911 from a soft client expects to reach local emergency services and not those of his or her home institution. However, in many (perhaps even most) such scenarios, connecting a user to local emergency services is difficult or impossible. Whereas how you address this problem will generally be based on a discussion with your general counsel and your local public-safety answering point, some possibilities to consider are:

- ❖ Mobile device location possibilities
- ❖ Various options to block 911 calls from mobile clients
- ❖ A pop-up screen with disclaimer and/or prompt for location information
- ❖ A fixed mobile client that forces emergency calls to go over the cellular network[4]
- ❖ Knowing which state's laws need to be complied with for communications that cross state boundaries (i.e., which E911 rules apply)[5]

Emerging Trends

Unified communications solutions that have the potential to greatly enhance and even transform communications during emergencies are becoming available. One solution currently on the market brings communications from any device into the same channel over an IP network. This enables everyone to communicate in real time regardless of whether the communication device is IP-based or not. For example, gateways are used to bring audio and data from radio systems into the system as IP packets. Combining this technology with the geographical redundancy and other advantages of cloud computing could result in emergency communications capabilities that are wholly independent of the organization's physical presence.

A major software vendor is focusing resources on the business need for emergency communication mechanisms that give emergency managers the ability to easily publish content and updates that make the information accessible to audiences from multiple end-user devices. The approach combines the vendor's tools to create an emergency collaboration platform.

Risks and Mitigation

- **Location identification:** The inherent diversity of the infrastructure supporting UC, especially in the case of mobile clients, creates significant location-identification challenges. Earlier this year the FCC adopted new wireless indoor E911 location-accuracy requirements,[6] but further development of standards is needed to ensure that location applications have the level of quality, reliability, and redundancy needed to support emergency location identification.
- **Power:** The same inherent UC infrastructure diversity creates power challenges. In particular, the nature of packet-switched networks requires a much broader resiliency and survivability approach. Unlike circuit-switched networks, the multipath nature of IP communications, combined with a more distributed power model, requires holistic backup power design, from core to edge to client.
- **Liability:** As a result of these "behind-the-scenes" challenges, the need to foster end-user awareness is obviously critical. In fact, enterprises that fail to do so likely incur liability for misrouted calls and/or location-identification failures. There are several methods for fostering the necessary awareness, improving safety, and mitigating liability. Some institutions simply disable the ability to place 911 calls from UC clients, along with an informative disclaimer to this effect. However, that approach is unnecessarily restrictive. Others force users to provide their location upon starting up their UC client. Unfortunately, this may not be sufficient for mobile clients on the move. And some, either in addition

to soliciting location information or in lieu of it, provide a click-through reminder/disclaimer that emergency calls may be misrouted and/or location information may be missing or inaccurate.

Note that these risks and mitigation strategies are focused on individual emergency communications. Mass notification systems have their own set of risks but rely on the diversity of communication modalities to ultimately reach their audiences.

Data Privacy, Security, and Compliance

Communications—and the data within those communications—now travel over shared digital media, are stored in different locations, and are often more vulnerable than they were in a legacy environment. Data security and privacy concerns, long an issue for other applications accessed over the IP network, must now be addressed for communication services. To many end users, the changes that come from the UC paradigms provide welcome conveniences. However, these feature enhancements inherently include potential security, legal, and privacy concerns. Understanding both sides of these issues is important when implementing change.

Emerging Trends

As more data are shared across an increasing number of repositories, institutions are considering encryption for data at rest and/or data-loss protection capabilities to reduce the risk of exposing regulated, sensitive, or confidential data. Some vendors are building these capabilities into their products, which could well become a differentiating factor when choosing solutions. The change in service architecture over the legacy communication environment will require staff who support the technology to develop new expertise in the area of data security and privacy and will require security experts to develop a better understanding of communications technologies and protocols. For example, technical experts with a background in legacy communication systems will require a deeper understanding of a range of security-related topics such as authentication, address spoofing, and vulnerability exploits.

Presence refers to the ability to proactively publish one's availability and willingness to communicate across a set of devices. Presence exploits the power of UC because it integrates multimodal forms of communication including, but not limited to, office phones, cell phones, e-mail, calendar, instant messaging, and videoconferencing by applying intelligent routing of real-time status updates, thus enabling end users to make better communication decisions. Presence in the context of UC can lead to a rich user experience, but the implementation process can be quite complex, given the number of devices, networks, and platforms involved. The complexity can result in mismanagement and a loss of privacy. It can also deter users from taking full advantage of UC. Privacy issues are typically addressed by allowing a high degree of user-defined control. Users can control how and when they communicate. Users can disable messaging functionality, restrict it to favored contacts, or select conditions in which they are detectable. User training is critical to protecting their privacy. These issues are exacerbated when leveraging federated presence.

As communication modalities continue to converge onto a single platform or tightly integrated platforms, new security, privacy, and compliance issues will continue to emerge. Social networking technologies in particular bear watching as they become a more inherent part of the UC applications suite.

Risks and Mitigation

UC technologies face the same risks inherent in an environment where systems are IP-based, accessible over the Internet, and increasingly connected with multiple endpoints for each user. Most security and privacy risks resulting from UC technology can be mitigated using the same firewall, encryption, and other data-security mechanisms used for other modern networked applications. The real risk is in users' and providers' lacking awareness of this shift and not applying the same risk mitigation, compliance measures, and lessons learned that have been developed for other network applications. This could lead, for example, to an increase in data-loss incidents, representing a step back for institutions that have made significant progress in containing and reversing a negative trend. Potential consequences of not applying risk mitigation and compliance measures include financial repercussions and the loss of reputation.

Call Centers and Consent

Call centers may be subject to state requirements when calls are recorded. States are identified as a "one-party consent" or "two-party consent" (sometimes called "all-party consent") state according to the level of agreement required by law before recording a phone call or conversation or conducting service observing. In a call center, one-party consent means that one of the parties, generally the employee, must be advised that calls may be recorded or observed. In a two-party consent state, both parties—the employee and the customer—must be advised. If a call center resides in a one-party consent state but initiates an outbound call to a two-party consent state, the calling center must apply the more strict state law and notify all parties to the conversation.

Privacy

Presence tools may introduce new personal privacy concerns, depending on the way those capabilities are deployed. Presence tools make information about the individual's availability for direct interaction accessible to a wide community. If end users do not have some control over how this information is made available to others, they may perceive the technology as too intrusive and choose not to use collaboration tools that incorporate presence information. The very reason for deploying these tools—to enable effective collaboration—could be undermined.

Location awareness (e.g., tracking the movement of Wi-Fi endpoints across campus) is a form of presence that delivers information about a device's physical location to another user or application. Geolocation information is derived from GPS satellites, cellular networks, and Wi-Fi hotspots and is *not* integrated with UC. Misuse of presence technology can result in a growth of nuisance communication including spam over IM (spim) or spam over IP telephony (spit). Unsolicited bulk messages can cause a denial of service and fraud and privacy violations. Presence technology that is improperly implemented or mismanaged can lead to harassment, stalking, surveillance, and illegal eavesdropping. Logging of location data also brings up privacy concerns, should these data become subject to e-discovery requirements.

Security

Personally identifiable information that is stored in an electronic form including voicemail and IM may be subject to discovery under e-discovery rules. Storage and retention of presence data is sometimes necessary for future recovery and analysis by regulatory authorities. Due to the transient nature of IM, investigators have a very short window to collect evidence. If IM archiving is unmanaged, compliance is not guaranteed. In the absence of central recording of UC communication, individual users should be advised against storing personal messages on institutionally owned devices any longer than necessary or risk public disclosure.

There is some ambiguity in regard to risk to confidential data in the UC domain. For example, providing a credit card number over the phone may be viewed as low risk, while providing the same information during a web conferencing session may not, given the readily available option to record the session. For similar reasons, displaying a license for purposes of ID proofing during a web conference may be considered less secure than faxing a copy of the document to another fax machine over an analog line—a means of data transmission that has been viewed as more secure than transmission over the IP network. Since the option to record web conference sessions exists for some environments, there may be a need to define compliance requirements at a level of granularity that will be very difficult for the average user to understand. Roughly 70% of Fortune 500 companies have adopted unified messaging as audio voicemail messages (often transcribed) delivered to e-mail inboxes. The 30% who haven't are generally in industries with high degrees of discovery in their business models, such as law, insurance, and so on.[7]

Compliance

New communications technologies result in a changed environment that forces institutions to make new decisions. Twenty years ago, e-mail made written communication easier and faster, but it shifted concerns from collecting and shredding paper to server storage policies and data encryption. VoIP, unified messaging, and unified communications are making voice and video communication easier and faster but are creating new challenges. A discussion that would have previously been analog and difficult to record is now digital and recorded with a single mouse click.

Concepts applied to other areas of technology translate to the UC environment. For example, FERPA defines "educational record" as any recorded information, including video and audio tape. Depending on content, recorded videoconferences and audio conferences may require the application of the same policies and procedures as other student records. Policies and procedures address such matters as disclosure to external parties and controls to limit access to authorized individuals. If the UC implementation includes cloud services, the nature of the contract with the vendor will determine whether it is appropriate to store information that can be classified as an educational record in the vendor cloud. Some institutions have required that the vendor acknowledge its role as a "school official" as defined in FERPA regulations. Other regulations that you should consider include:

- **ADA:** The Americans with Disabilities Act requires reasonable accommodations (e.g., a modification or adjustment to the status quo inherent in the program or activity) to allow a qualified person with a disability to participate fully in the educational or academic programs and activities of the university.
- **Clery Act:** The Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act[8] is focused on campus safety and contains public-safety notification requirements that may need to be put into place in UC.
- **FISMA:** The Federal Information Security Management Act[9] focuses on cybersecurity risks for the federal government. For institutions, this includes privacy requirements for federal government-funded research, such as physical segregation from the rest of your networking infrastructure through a FISMA-compliant ISP.

- **HIPAA:** The Health Insurance Portability and Accountability Act[10] protects health information privacy. Health-related information may require encryption; when looking at all the new places where UC data are being stored, this needs to be taken into consideration.
- **ITAR and the EAR:** International Traffic in Arms Regulations and the Export Administration Regulations are export control regulations run by different departments of the U.S. government. Both are designed to help ensure that defense-related technology does not get into the wrong hands.

Data Storage

In a UC environment, data storage for communications content represents a new challenge, relative to traditional voice services. In the traditional or legacy environment, such content has been much more ephemeral and fairly contained within the voice infrastructure and not necessarily readily available over the IP network. As UC capabilities such as unified messaging and web conferencing are deployed, the content may reside within multiple applications and locations (on premises or in the cloud) and on multiple endpoints. The proliferation of IP-connected devices is an important case in point as the types of data being stored on endpoints expands to include voice and video content. The type and number of unmanaged endpoints (e.g., Apple Watch and the Internet of Things) may have already reached a level where mobile device policies in place are no longer relevant.

Ease of recording and distribution across multiple repositories is an important factor to take into account. Huge storage quotas may pose additional and separate challenges such as an exponential increase in the volume of communications data retained for any given period of time. Some file formats may not lend themselves well to e-discovery (e.g., WAV versus text), raising the potential need for additional capabilities such as speech-to-text indexing. To the extent that the attack surface associated with this type of data increases, the issues described above on data security and privacy are accentuated.

Emerging Trends

Data-retention practices depend on state laws, local requirements, and institutional policy. Institutional guidelines around these topics will be important. Many institutions may not have any history of applying data-retention policy to content formats such as voicemail and video recordings. Given the rapid rate of technological change, institutions should expect to review these guidelines on a regular basis and proactively identify new areas to apply them.

Work teams that have grown up with traditional voice technologies must come up to speed to understand how the new environment changes how they interact with the data and how the changes impact their role as data custodian. Staff who manage on-premises storage repositories or who monitor and manage cloud-based storage quota consumption must be aware of the coming changes and be prepared to respond with corresponding changes in their operational procedures. For example, e-discovery requirements may drive such operational changes as speech-to-text indexing. Call tracing and tracking may require the implementation of new processes and procedures.

Risks and Mitigation

The greatest risk for an organization is not having reviewed existing policies, vendor contracts, service level agreements, and operational practices in light of this new model. Acknowledging the increase in the number of data storage locations, including personal end devices, is the first step. Inattention to this reality would increase the risk of:

- Data leakage and exposure to unauthorized parties.
- Reduced effectiveness in responding to e-discovery requests.
- Failure to adhere to regulatory and policy requirements when data repositories have not been inventoried.
- Data storage requirements that outpace budget allocations.
- Increased support load related to e-discovery requests for these data and requests to transfer these data from one staff member's account to another's in cases of sudden termination or when the department has not followed good offboarding procedures during routine staff departures. This support load already exists for text-based services such as e-mail and document-sharing services such as Box and OneDrive for Business.

Conclusion

As institutions deploy unified communications capabilities, models developed for managing risk in the world of traditional telephony must be modified to align more closely with those developed for managing risks associated with other applications accessed over the IP network. Many of the new communication risks introduced by UC technology have existed for other areas of IT for some time, with each institution implementing necessary controls and measures to mitigate them. Changes in the mode of communication itself from telephone conversations to the multiple modes available with today's UC solutions requires a careful reconsideration of the institution's position on communications during emergencies. The conversation must focus on the current reality, where most individuals are multiply connected and do not view the traditional telephone as the primary or preferred method of communication, while regularly consulting regulatory requirements for the specific jurisdiction. Privacy issues raised by new features and functions, such as presence and the distribution of communication content across multiple devices, must be addressed as the institution implements unified communications.

Authors

Special thanks go to the following ECAR-Communications Infrastructure and Applications (ECAR-CIA) Working Group authors of this report.

Charles R. Bartel
Assistant Vice President and CIO
Duquesne University

Andrea Beesing
Assistant Director, Cornell Information Technologies
Cornell University

John Callahan
Director of Infrastructure Services
Willamette University

Richard Hach
Director, Client Services, Special Projects and Initiatives
Virginia Tech

James A. Jokl (Co-Chair)
Associate Vice President and Chief Enterprise Architect
University of Virginia

Mark Katsouros (Co-Chair)
Director, Network Planning and Integration
The Pennsylvania State University

Timothy Lance
President
NYSERNet

Ryan Lenger
Manager, Enterprise Communication and Collaboration
The University of Iowa

Anne M. Phillips
Assistant Director, Telecommunication Systems, Infrastructure Planning and Facilities
Michigan State University

Steve Troester
IT Director
The University of Iowa

Felicia Watson
Assistant Director
University of Washington

Acknowledgments

Additional thanks go to the following ECAR-CIA Working Group members: Douglas Carlson, Associate Vice President, C&CS, New York University; Randy Monroe, Assistant Director, Unified Communications, Carnegie Mellon University; Kathleen Murphy, Service Manager, University at Buffalo–SUNY; and Steve Updegrove, Senior Director, Telecommunications and Networking Services, The Pennsylvania State University. For more information about this paper and ECAR working groups, contact Karen A. Wetzel, Program Manager, EDUCAUSE.

Citation for This Work

Bartel, Charles R., et al. *Unified Communications in Higher Education: Responding to New Risks*. Working group paper. Louisville, CO: ECAR, November 15, 2015.

Notes

1. For a complete definition of *unified communications* and a discussion of the differences between legacy and unified communications, approaches to this shift, and several themes that have emerged in this area, see Charles R. Bartel et al., *Improving Institutional Collaboration through Unified Communications: A Study of Current Implementations*, ECAR working group paper, December 12, 2014.
2. James A. Jokl, *Distributed Antenna Systems: ACTI Briefing Note*, ACTI briefing note, October 11, 2012.
3. Federal Communications Commission, "911 Wireless Services."
4. Fixed–mobile convergence is the ability for dual-mode devices (e.g., iPhone) to switch between wireless and cellular service. For more information, see fixed–mobile convergence.
5. Enhanced 911, or E911, is mandated in the US by the Wireless Communications and Public Safety Act of 1999. It is a system that "links emergency callers with the appropriate public resources." See also "Enhanced 9-1-1," *Wikipedia*.
6. See FCC Adopts New Wireless Indoor E911 Location Accuracy Requirements.
7. Steve Blood and Sorell Slaymaker, *Critical Capabilities for Corporate Telephony*, Gartner, October 14, 2014.
8. See Summary of the Jeanne Clery Act and also Mark Katsouros, "Emergency Communications Management and the Clery Act," *EDUCAUSE Live!* webinar, February 28, 2013, and Mark Katsouros, *Emergency Notification Strategy*, ECAR working group paper, April 8, 2014.
9. See Federal Information Security Modernization Act (FISMA).
10. See Health Information Privacy.