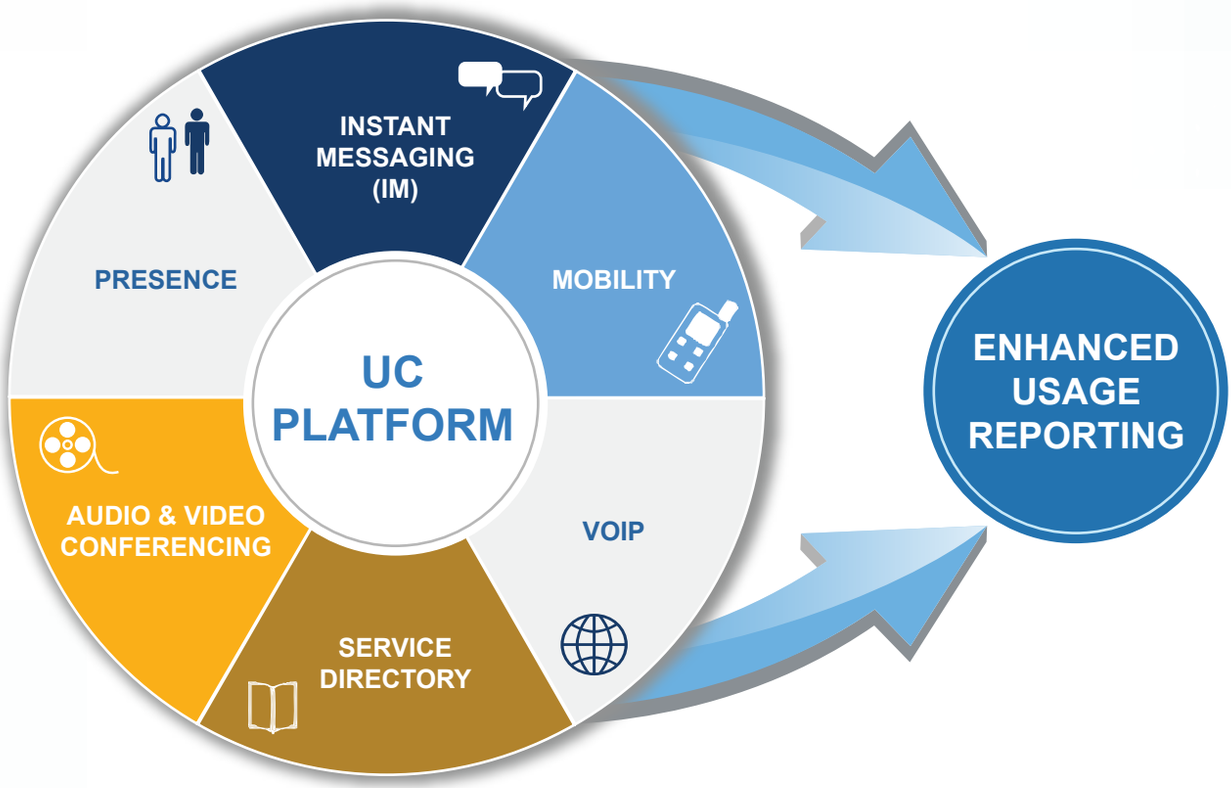
WHITEPAPER

Unified Communications (UC)

The Price of Productivity - Mitigating the Risks of Unified Communications Deployments



Enterprises are incorporating UC at a rapid pace due to its low-cost value proposition and expected increase in productivity. Are there "hidden costs" that are not being fully appreciated? Do they outweigh the benefits? The risks of implementing a UC solution aren't always obvious and go beyond a simple errant text or instant message (IM), including:

- Legal Liability
- Regulatory Compliance
- Loss of Intellectual Property
- Loss of Productivity: Misuse of Corporate Assets

How do you mitigate these risks to ensure that UC deployments have a positive impact on the firm?

A successful UC deployment involves ongoing and seamless monitoring and reporting on UC asset usage. Critical to a successful long-term UC strategy is comprehensive visibility and actionable insights regarding misuse, abuse and intellectual property sharing. An Enhanced Usage Reporting platform can mitigate the risks associated with a UC deployment and allow the firm to reap the productivity gains from UC with confidence.

WHITE PAPER

UC Deployments Are Increasing – So Are the Risks

"The Unified Communications-as-a-Service (UCaaS) market is expected to grow from $2.52 billion in 2013 to $7.62 billion by 2018, at an estimated CAGR of 24.8%." – Unified Communications as-a-Service (UCaaS) Market: Advancements, Emerging Applications, Business Models, Technology Roadmaps, Global Forecasts & Analysis (2013 - 2018) - Markets and Markets.

> ***"There will be a bit of an education process that we will need to go through with the customers but I'm convinced "reporting" is going to become table stakes."***
>
> - David Walsh, CEO of GENBAND

While the concept of UC has been around for decades, its acceptance has accelerated as VoIP-enabled communications took hold. ***"The solution has really only just begun to mature, as have the risks."*** The well-documented mobility trend, fueled by the Internet of Things (IoT), will only add to the increased acceptance and deployment of UC. **Can you track UC Usage and protect your firm? What is the cost of a security breach?** These questions and other security-related UC implementation issues are challenging users and service providers.

The Risks and Potential Threats of UC Deployment

Unified Communication deployments are expanding rapidly. Yet, many enterprises are blissfully unaware of the significant security, abuse and misuse exposures inherent in these deployments. The same UC tools that enhance productivity can be easily used to circumvent firewalls and share intellectual property. ***"Lack of visibility, data and analytics allow for employee abuse or misuse of UC platforms."*** A few public examples of the failure to uncover misuse exist and they will only increase.

Well-Known Telecom Incumbents Are Not Immune

A high-powered executive has been fired after a $100 million lawsuit was filed claiming he sent racially offensive images on his work phone. The images in question were found on the executive's phone by an assistant who was asked to transfer data to a new phone, according to the lawsuit – **"There is no place for demeaning behavior within the company and we regret the action was not taken earlier,"** a company spokesperson said.

While this executive may have committed the offense, it is the company that will ultimately pay the price for its lack of visibility and oversight of its corporate UC assets. The company is being sued at the corporate level and it has deep pockets.

No Easy Wins for Women in Discrimination Lawsuits

A dating app co-founder sued her own company and parent company, alleging the CEO and co-founder subjected her to "horrendously sexist, racist, and otherwise inappropriate comments, emails and text messages," before firing her. She and the parent company settled out of court for an "undisclosed sum." Forbes reported **she received "just over $1 million."**

Might the company have been better able to defend itself if it had retained all text messages, and not had to just selectively defend against those texts proffered by the Plaintiff?

Regulatory Compliance and Legal Liability

As noted above, internal security breaches can cost companies millions each year. Monitoring of corporate communication assets is a key component of risk management. Moreover, the management, monitoring and memorializing of these assets and communications are often the law.

Sarbanes-Oxley

The rules governing the use of IM in the financial industry are often overlooked as firms work diligently to comply with the Sarbanes-Oxley Act. Sarbanes-Oxley impacts many areas of a business, including IM. **In fact, even firms that specialize in compliance often overlook IM**, yet the SEC has stated that instant messaging is bound by the same guidelines as email.

The SEC regulation SEC 17 CFR 240, which came into effect in May 2004, requires that all communications between stockbrokers and clients, including e-mail and instant messaging messages, be retained for three years and be easily accessible for the first two years (Sarbanes-Oxley: Implications for Document and Message Storage – Info Tech Research Group). The rules do not specifically state that ***firms are required to review or approve instant messaging content. However, regardless of the content, the message must be archived.***

HIPAA

In an article written by Arlene F. Baril, MS, RHIA, for ADVANCE, a producer of multimedia resources and education services to the healthcare community, Baril maintains that there are a number of potential communications-based HIPAA violations with which to be concerned. A facility that does not follow these rules can be excluded from participation in the Medicare/Medicaid programs. Penalties can escalate to $100,000 in fines and up to 5 years in prison if the offenses are committed under false pretenses, and up to ***$250,000 in fines and up to 10 years in prison if the information obtained is found to be used for commercial advantage, personal gain or malicious harm***.

Some of the worst cases of HIPAA violations involve healthcare workers' snooping into the private files of patients to learn information they have no need to know. At times, UC assets are then used by employees to disseminate such information illegally. This is common for celebrity patients. The records of Tammy Wynette and Farrah Fawcett, for example, were viewed and sold to the media.

A federal court handed down the first criminal sentencing for this type of offense in April 2010. Huping Zhou, a former researcher at the UCLA School of Medicine, accessed high-profile patient files more than 300 times, including the records of Sharon Osbourne, Barbara Walters, Elizabeth Banks, Leonardo DiCaprio and Anne Rice. He was sentenced to 4 months in a federal penitentiary for his "lack of respect for patient privacy."

Dodd-Frank Act

Perhaps the most extensive and significant electronic record retention requirements are contained in the Dodd-Frank legislation and regulations. According to the legislation, ***financial institutions must ensure that they have the capability to archive and maintain all types of electronic communications***. Therefore, the installation of text message, voicemail, instant messaging, voice call and email archiving and reporting is a requirement for many financial institutions.

WHITEPAPER

Mitigating the Problem with Intelligent Communications Management (ICM) – Enhanced Usage Reporting (EUR)

Fortunately there are pioneers in back-office expense management and telecom asset management dedicated to uncovering potential issues as methods of communications evolve. They have not only monitored and reported on the potential problems associated with UC implementation and asset misuse – they have also worked to mitigate those issues.

Today ***enterprises can install their favorite UC platform, in concert with an Enhanced Usage Reporting solution that effectively mitigates these risks***, protecting their communications environment.

ICM Enhanced Usage Reporting (EUR) is an integral tool in Avotus' Intelligent Communications Management (ICM) program. EUR integrates, tracks and reports on usage for Unified Communication services. ICM EUR allows communication managers to gain unprecedented visibility into the full suite of Unified Communication features, including: IM, Presence, Voice, Wireless and Video Conferencing with one unified tracking and reporting platform.

Deployed as either a cloud-based service or on-premise, Avotus' ICM Enhanced Usage Reporting delivers unmatched visibility into your corporate communications, improving overall UC asset usage visibility, reporting, monitoring and security across your wireline, wireless, VoIP, UC and legacy platforms. Key enterprise protection, misuse and prevention features and advantages include:

Features

- Visibility into the departments contributing most to telecom expense and broadband usage
- Uncovering security, compliance and other potential asset misuse or abuse, gain visibility into UC file-sharing, screen share and instant messaging content – full audit trails on each message
- Optimization of your UC investment by identifying under-utilization, training opportunities and unsecure platforms operating within the firewall
- Regulatory Compliance with HIPAA, Sarbanes Oxley and Dodd-Frank. Archive, monitor and search for instant messages in compliance with (SEC, FINRA, SOX, IIROC, FSA) privacy laws
- Response to litigation with accurate information about UC usage
- Online search, monitoring and reporting tools to enable compliance review, surveillance, monitoring, HR management and internal policy enforcement - rapid search capability to find & retrieve any message in seconds
- Better manage growing and diverse fleets of mobile, tablet and other communication devices
- Integration, management and control telecom investments across multi-vendor/multi-site environments
- Tracking and exception reporting across all UC features detects abuse and ensures compliance with corporate guidelines and regulatory requirements
- Hosted archive provides secure, centralized offsite storage in SSAE 16 Type II Data Centers
- Bill back - usage charges to departments, cost codes or employees

WHITEPAPER

Advantages

- **Regulatory Compliance** — Financial industry regulations such as Sarbanes-Oxley, Dodd-Frank, HIPAA and many others require all electronic business communications to be archived and monitored, including instant messages. It's the law.
- **Visibility** — Avotus' EUR provides comprehensive visibility, supervision and monitoring tools that provide detailed reviews and reports of all communications, including instant messages — facilitating supervision and HR policy enforcement.
- **Security** — Having a UC communications archiving and monitoring solution in place is the best way to help mitigate the risks of UC use. When every communication is captured and stored, liabilities are reduced.
- **Convenience** — With Avotus EUR you can search and retrieve any past communication quickly and easily — no matter when – within minutes.

Conclusion

A potentially serious problem exists for any organization that deploys a UC solution. Unfortunately, some are failing to recognize the risks and address them with a viable solution such as Enhanced Usage Reporting. This opens those enterprises and service providers up to serious and possibly crippling effects of unchecked and unmonitored communications. From internal IM misuse to the real possibility that proprietary material may be shared via unmanaged employee devices and file-sharing, it is imperative that businesses be protected. What's more, proper visibility enables enterprises the ability to observe UC usage that is inconsistent with corporate policies or the job functions of individual employees and to spot "training" opportunities for employees who are over- or under-utilizing the system in a manner that might require intervention. True efficiency, visibility and protection can only be obtained via an Enhanced Usage Reporting solution.

About Avotus

With more than 30 years of industry experience, Avotus is the award-winning provider of **Intelligent Communications Management (ICM)** solutions. ICM solutions enable users to optimize, manage and protect against misuse and abuse of their critical investments in telecom and technology. Avotus' ICM lifecycle can be deployed in a manner that allows each engagement to self-fund the next, while putting cash on the client's bottom line at each step. ICM solutions include: Enhanced Usage Reporting (EUR) for Unified Communications, Expense Management with ITAM Robot (EM), Intelli-Sourcing and Wireless Management. Avotus and its partners serve more than 1,000 clients in North America and around the world, many of which are industry-leading Fortune 5000 companies. ICM is Avotus' Intelligent approach to managing wireline and wireless assets, and a safeguard for your next-generation communications solutions.

Appendix

As we push further into the 21st Century, businesses generally recognize, for many, the necessity, and for others, the potential benefits, of a well-tailored record retention, maintenance, production and destruction program (a "**Records Retention Program**"). Maintaining electronic records lies at the heart of records retention requirements and programs. The past decade has been marked by the proliferation of different forms of electronic communication, with the old business workhorse, e-mail, now regularly supplemented by the use of instant messaging to conduct business. The below information focuses on why many businesses must, and others should, include a process for retaining their workers' business-related instant messages ("**business IM**") in their Records Retention Program.

For companies doing business in the U.S., the regulatory aspect of business IM record retention varies significantly based on business size and industry:

- Smaller private companies not involved in the financial industry can assess their requirements partly from a basic controls and risk management perspective, partly by looking to the applicable regulations that may apply to their specific business, and partly with a focus on the requirements of the Federal Rules of Civil Procedures, which will apply if and when the company faces a dispute brought in a federal court. In sum, these court rules require business IM to be stored and produced if litigation or investigations are imminent.

- Provisions of the Sarbanes-Oxley Act require U.S. publicly traded companies with revenues in excess of $75 million, and certain private companies, to maintain business records—broadly defined as any material that contains information about the company's plans, results, policies or performance—for five years, and longer in some circumstances. So, these companies must retain business IM.

- A related issue is security of business IM, and companies in the health care industry must focus on meeting the requirements of HIPAA in handling patient information.

- Companies involved in the financial industry face a host of different regulations that, generally speaking, require retention of business IM, usually in a non-rewritable, non-erasable format (also referred to as "Write-Once, Read-Many" or "WORM" format) to prevent alteration, and also may frequently require that the company have the ability to review business IM for supervision and compliance purposes. For example, here is a NASD (now FINRA) statement from 2003 (by Mary Shapiro, who later chaired NASD/FINRA and the SEC):

  "NASD recognizes that instant messaging is becoming increasingly popular as a real-time method of communicating and we want to be clear about our expectations for its use. Firms have to remember that regardless of the informality of instant messaging, it is still subject to the same requirements as e-mail communications and members must ensure that their use of instant messaging is consistent with their basic supervisory and record-keeping obligations."

A recent headline grabber in the area of instant messages record retention is FINRA's fining Barclays Bank $3.75 million at year end 2013 for systemic electronic records retention failures, including a finding that Barclay's "failed to properly retain approximately 3.3 million Bloomberg instant messages from October 2008 to May 2010." FINRA specifically cited the requirement to keep business-related electronic records in non-rewritable, non-erasable format to prevent alteration. So, the failures did not necessarily represent a failure to maintain records at all, but rather a failure to retain the records "properly." Less of a headline grabber, but still not nickels and dimes, in late 2014, the CFTC fined a former CBOT floor broker (an individual) $200,000 for

record-keeping violations that included failing to keep complete records of business-related instant messages. Less recently, multi-million dollar fines and sanctions have been levied by both courts and securities regulators for failures to retain or produce electronic business records, in both financial industry regulatory actions and non-financial industry lawsuits.

In the U.S. federal court process, sanctions are routinely imposed on parties that fail to produce electronic records—simply lacking the capacity to retain or produce the records typically is not an excuse. Such a failure of capacity also puts a party in an unenviable position: The other party may have done a better job retaining the relevant communications and may end up in a position (whether properly or improperly) to control what part of the record is produced. This potentially places the party who lacks complete records at a significant disadvantage. Depending on the circumstances, court sanctions for failing to produce business records can include "spoliation inference" (the jury is instructed that it may assume that the lost evidence, if available, would have been unfavorable to the spoliator), fines, barring a party from making an argument or introducing evidence, even a default judgment or dismissal of a case.

The path to recognizing the need to retain business-IM is similar to the path previously followed for business emails: A new technology develops and is adopted for business purposes. Lagging behind adoption comes regulatory focus and the technology required to properly retain, store, and organize an initially overwhelming volume of a new form of data. As the business reality sinks in that most laws and regulators will not differentiate between different formats of business records when they write and interpret the rules for records-retention, technology service providers then step in with products and services to fill the records retention gaps: Today, businesses can choose among products and services designed to provide a clear path to implementing a Records Retention Program that include business IM and that can be designed both as an internal control and risk management tool and as a means to complying with applicable laws and regulations.

This summary has focused on reasons for including business IM in Records Retention Programs for companies doing business in the U.S. A partial list of U.S. regulations that affect different types of businesses follows. A survey of non-U.S. law is beyond the scope of the data included here; however, a partial list of non-U.S. regulations that may affect companies doing business in several non-U.S. jurisdictions is also set out below.

Some U.S. Federal Laws that Require Retention of Instant Messages that are Business Records:

Federal Rules of Civil Procedure. The Federal Rules of Civil Procedure do not distinguish between information contained in word processing documents, contained in emails, and contained in instant messages. Information must be stored and produced if litigation or investigations are imminent. So, if business is conducted using instant messaging, there is the same need to archive and be able to produce instant messages that exists with respect to email and other documents.

Sarbanes-Oxley. Under this Act of Congress, publicly traded U.S. companies with revenues in excess of $75 million and certain private companies must maintain business records—broadly defined as any material that contains information about the company's plans, results, policies or performance—for five years, and longer in some circumstances.

Securities Exchange Act Rules 17a-3, 17a-4, NASD Rules 2200, 2310, 2711, 3010 and 3110 (replaced or being replaced by FINRA Rules 2111, 3110, 4511, etc.) Broker dealers are subject to multiple rules requiring maintenance of instant messages utilized for business, with supervisory and compliance review capability.

CFTC Regulations 1.35 and 1.31. Futures commission merchants, introducing brokers and members of a designated contract market are required to keep business records, including records of all trade information, and the CFTC has issued guidance to state clearly that the rules "do not distinguish between whatever medium is used to record the information covered by the regulations, including emails, instant messages and any other form of communication created or transmitted electronically."

Non-U.S. Laws that May Require or Guide Retention of Instant Messages that are Business Records:

Canada: Rule 30.02 of Ontario Rules of Civil Procedure; Bill 198 ("Canadian SOX"); Personal Information Protection and Electronic Documents Act (privacy).

Europe

European Union Data Protection Directive 95/46/EC; Euro-SOX (Statutory Audit and the Company Reporting Directives); MiFID (Markets in Financial Instruments Directive); Numerous member-country-specific laws and regulation.

Asia-Pacific

Australia: Corporate Law Economic Reform Program (Audit Reform & Corporate Disclosure) Act 2004, (commonly called CLERP 9); The Privacy Act 1988.

India: Section 120 of the Indian Companies Act of 2013, and the Companies (Management and Administration) Rules of 2014; Right to Information Act.

Japan: J-SOX (part of Japan's Financial Instruments and Exchange Law); JPIPA (Japanese Personal Information Protection Act).

Singapore: Companies Act.

Important Disclaimer

This information should be referred to for general information purposes only. These materials do NOT constitute legal advice or other professional advice, and you may not rely on the contents as such. For legal advice related to the topics covered above, you should retain competent legal counsel to advise you.