

Secure Communication Principles & Tips By Salt Communications

Nicole Allen | August 15, 2022



Salt Communications Interview with [Safety Detectives](#).

You hear about data leaks and [cyber attacks](#) almost daily, and nevertheless so many companies still don't understand why it's important to ensure they are protected against these attacks.

Many have rushed over digital communication channels during the recent pandemic without proper knowledge and understanding of the risks involved, which explains the rise in data breaches and cybercrime in general.

To discuss how organisations should approach communication security, we invited **Nicole Allen, the Senior Marketing Executive at Salt Communications**, a company specialised in protecting the confidentiality of sensitive enterprise information with their secure communications platform.

Business owners and normal people alike cannot ignore these cyber threats anymore, so we asked Nicole to explain why communication security is crucial nowadays and how to better protect your sensitive conversations.

Please describe the story behind Salt Communications: How did it all start, and how has it evolved so far?

Salt Communications, headquartered in Belfast N. Ireland was formed in 2013 by a group of tech entrepreneurs with a shared history in enterprise security, telecoms, network optimisation and app development. After the release of the iPhone in 2007 and the Android in 2009, the founders of Salt observed a significant movement towards mobility. It was obvious that communication applications were altering how people used their phones, but they were primarily designed with consumers in mind. Salt Communications' founders recognised that there was a chance to create a system that provided all the appealing features of consumer messaging apps while concentrating on an organisation's security. This would enable organisations to maintain compliance, have complete control over their system, and, of course, keep their private communications confidential.

Salt has evolved to a stage where we work with some of the largest organisations in the world across many different industries who all see the significance of using a secure communications system. Our customers include global law firms, financial institutions, defense and security clients, oil and gas companies and large enterprises.

What are the key features of your security platform?

Our key features within our security platform are secure voice and video calling, messaging, broadcasting and image or file transfers for busy professionals who need to make important decisions on the move.

We also offer unique features such as the ability to restrict users from taking screenshots, the ability to prevent users having the capabilities to download documents & images and the ability for users to purge messages from their device & all recipients devices too – a function that can be done manually, or have a timer setting.

What's crucial for many of our larger clients is the flexibility of deployment. Salt understands the need for complete control so we go above and beyond to ensure the system can be white labelled, hosted in the customers infrastructure and integrated with the clients' pre-existing systems.

What are the most common risks caused by a lack of security in communication?

Hackers are looking for any way to access smartphones and tablets as they become commonplace companions. Many people assume that iPhones and Android devices are secure by default, but in truth, security settings adjustments must be made by the user. Some of the most common risks are that hackers can acquire access to a nearby mobile device in less than 30 seconds with the correct tools, mirror the device so they can see all communication methods on the device if not using a secure business communications app or implant malware so they can steal data from it whenever they want.

Another common risk is consumer app vulnerabilities. Consumer applications are already being used by many people in their jobs. Although there are many great, free tools available for consumers to utilise, there are several long-term risks that businesses need to be aware of. From theft or malicious interception, service dependability issues, and availability issues are among the risks. Consumer tools frequently do not offer robust enough SLAs and may not offer sufficient support for problems organisations may run into. Consumer-grade communication tools can also open up a wealth of security issues – something that enterprise communications systems are designed to prevent

Did you notice a change in the general awareness of cybersecurity since the Covid outbreak?

Yes – quite drastically actually. As many people know, the Government limitations put in place in reaction to the coronavirus pandemic encouraged workers across the globe to work from home where possible. As a result, technology continues to play a bigger role in both our personal and professional life. However, due to this rush to get systems in place, organisations have rarely gone back re-evaluate how these systems actually work long term. They chose productivity over security, and that continues to leave a security gap.

Despite this increase in technological demand, it is apparent that some organisations still do not offer a "cyber-safe" environment for remote working. While business meetings were once held in person, they now mostly occur online.

With this in mind we noticed many more organisations taking an interest in protecting their devices against cyber attacks and how they can do their best to protect themselves and the workforce. A lot of this came down to the fact that many people were now working off their home WIFI and personal devices for work matters.

A great deal of confidential information is now being passed through personal devices and networks which don't have anywhere near the same amount of protection as corporate networks. As a result of this many organisations have put communication policies in place, continually monitor systems, educate employees more on the risks and are using a secure communication system for all confidential matters.

What are the best practices for data protection against cyberattacks that every business should apply?

To start off with, get rid of the *'it won't happen to me mentality'* it can and it likely will. Threat detection has gotten harder since attackers are always coming up with new ways to access sensitive data. Furthermore, privileged and remote users are now among the top insider actors due to the recent trend of remote work and the granting of privileged access to numerous employees. One of the best practices would be to employ a people-centric cybersecurity approach when communicating throughout the organisation. Your strongest security shield or your worst security threat can both be people.

Since hackers frequently employ people as entry points, a technology-centric approach to cybersecurity is no longer sufficient to provide complete protection. Therefore, the greatest strategy for reducing risks associated with people is to take a people-centric approach. The employees themselves are a crucial perimeter in people-centric security.

Another best practice is having a [secure communications](#) system which allows employees to communicate safely internally and externally. By giving organisations the power to manage their own communications, many of the hazards other businesses face when sharing sensitive information via mobile devices are reduced. When all of this is taken into account, your company's data is always protected from outside intruders.

It's essential to consider both the threats that your employees could pose and how important they are to your cybersecurity. The two most important factors to take into account while attempting to defend your cyber environment are training and workforce monitoring to protect your confidential data at all times.

What can normal users do to secure their communications?

The truth is that anyone using consumer apps for their communications is never safe. It is difficult to remain secure, many are being pointed towards Signal instead of WhatsApp, this system has the same vulnerabilities just with less global users. Many consumer apps advertise that they are 'encrypted' but encryption alone isn't enough. Due to the instability and lack of control of these apps they pose a risk to anyone's communications who uses them. That's why companies need to take control of their communications, because there's no way for the consumer to do this.

How do you envision the future of your industry and your company?

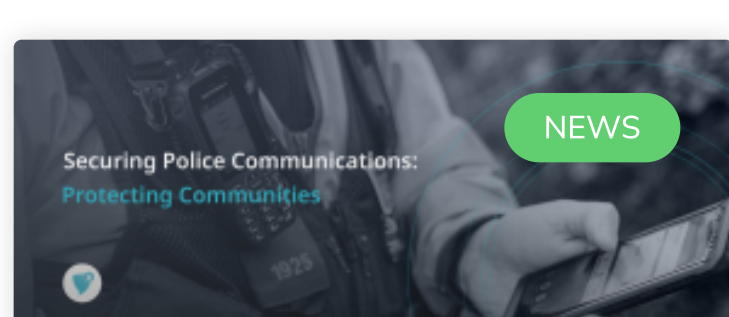
Salt Communications strives to be a globally recognised cybersecurity leader, and the go to secure communications platform for organisations across the globe, both in the public and private sector. With continuous reports around the vulnerabilities of consumer systems, and the business continuity issues faced with systems tightly linked to the companies active directory, we believe the requirement of secure communications will continue to rise, and demand levels will continue to rise also.

We are working hard on many exciting features and projects in our pipeline that will all be announced very soon! In the meantime we will always be working with our clients to facilitate what their day to day needs are within their communications and how we can continue to help secure their communications. Keep an eye out for what's coming up!

Share This Post

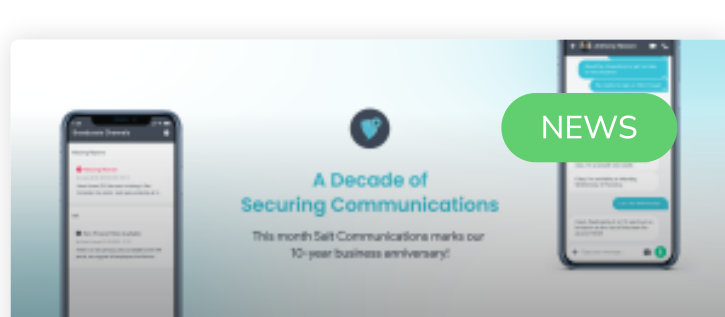


Explore More




Securing Police Communications: Protecting Communities

Probably now more than ever, secure communications are crucial for Policing and the communities they serve. The ability to successfully communicate with co-workers, superiors, other




A decade of Securing Communications

What a thrill to share the last decade with you! This year is marked in bold for everyone at Salt Communications. We will be marking



Salt Communications to attend Lexpo 2023

Salt Communications – a Northern Ireland based cybersecurity company who provide secure mobile communications solutions to some of the largest Law Firms worldwide are attending



4 Reasons Why Not to Use WhatsApp for Secure Communications

Don't settle for just using WhatsApp for secure communications. Check out these 4 reasons why you should consider a WhatsApp replacement. WhatsApp is a communications

Newsletter

 Your Email Address

SUBSCRIBE

Continue to build your cyber knowledge by subscribing to Salt's bi-weekly newsletter which includes cybersecurity and mobile security news, as well as Salt Communications' articles, announcements and [Webinar](#).

Solutions

Critical Infrastructure
Remote Working
Incident Response
Client Communications
VIP Protections

Industries

Police
Military
Government
Legal
Enterprise
Financial

Company

Contact Us
About Salt
Salt FAQ
Careers
Videers
Webinars
News & Blog
Feature Comparison
WhatsApp Replacement

Salt News

Press Release
Release Notes
Awards
Buy Salt License

Social

Find us on social media

