RANSOMWARE RESILIENCE SUMMIT USA

Benchmarking ransomware resilience and business continuity planning

Q&A: ROLAND CLOUTIER CHIEF SECURITY OFFICER TIKTOK AND BYTEDANCE

Kisaco Research

Roland Cloutier

As Global Chief Security Officer of ByteDance and TikTok, Roland Cloutier brings an unprecedented understanding and knowledge of global protection and security leadership to one of the world's leading media, social, and technology companies. He oversees the company's information protection, risk, workforce protection, crisis management, and investigative-security operations worldwide. Before joining ByteDance and TikTok in 2020, Cloutier spent about 10 years as CSO at payroll-services firm ADP. Prior to ADP, he was CSO at data-storage vendor EMC (now owned by Dell). Cloutier started his career with over a decade of service to the US Air Force and US Depts. of Defense and Veterans Affairs. In 2015, he authored and published a business book, "Becoming a Global Chief Security Executive Officer."

Roland Cloutier
Global Chief Security Officer
ByteDance/ Tik Tok

You recently launched the #BeCyberSmart campaign at TikTok as a part of Cybersecurity Awareness Month. What was the driver for doing this?

At TikTok, we believe everyone benefits from a safer and more secure world. For Cybersecurity Awareness Month and all year long, we're inspiring our diverse global community to make good choices and stay safe online. That's why we launched #BeCyberSmart, a campaign championed by the National Cyber Security Alliance (NCSA) and industry-leading experts on how we can all create a culture of cybersecurity. We're always inspired by creators fueling #LearnOnTikTok, and it was exciting to launch a new @TikTokTips video series on ways to spot and defend against common cyberthreats. The series features TikTok creators and employees, including touring comedian @alex_falcone telling tales of cyber crimes and how to #BeCyberSmart.

We also want to uplift the next generation of leaders. While the pandemic hit many industries hard, cybersecurity skills have never been needed more. Over 3 million cybersecurity jobs went unfilled last year. We're providing tools, training, and encouragement to inspire more people to get into cybersecurity. We've also been strengthening our security team at TikTok.

We're actively recruiting for over 300 roles across 19 different disciplines, because securing a platform that brings joy to over 1 billion people is a job that's never done.

Ransomware attacks have significantly driven cybersecurity's public profile. How have you seen this impacting internal support for cybersecurity initiatives, budgets and overall awareness with businesses?

Ransomware attacks have surged 311% in the past year with a business now being attacked every 11 seconds, and the threat landscape is constantly evolving. At TikTok, the safety and security of our global community is always a top priority. We know that staying ahead of next-generation cyber threats requires bolstering the security and integrity of our platform and business operations on an ongoing basis. Critical to that effort is partnering with the world's best researchers, academic scholars, and independent experts to test and validate our own defences.

In the past year alone, we've strengthened our global security organization and established global Fusion Center operations in Washington DC, Dublin, and Singapore. We've earned ISO 27001 certifications in the US, UK, Ireland, Singapore, and India for investing in the people, processes, and technology to keep our community safe.

We continue to partner with leading organizations like the National Cyber Security Alliance to inspire leaders of the future and encourage people of all backgrounds to #BeCyberSmart.

While celebrating our 1-year anniversary with HackerOne and the evolution of its Internet Bug Bounty (IBB) program, we worked to spotlight the top ethical hackers helping TikTok pioneer new defenses to protect over 1 billion people worldwide. Our comprehensive scope and commitment to transparency is what keeps drawing new hackers to the program.

What advice would you give to CISOs looking to raise cybersecurity awareness within their business and promote a 'cyber risk' culture?

People are the foundation of any organization, and security is a team sport. At TikTok, our employees are our first line of defense. We're focused on creating a culture of security within our organization. That includes developing an internal video game to educate employees on cybersecurity and sharing @TikTokTips videos to encourage strong passwords, multi-factor authentication, and ways to spot phishing attempts. We also host a regular "Mission Possible" series with programming to engage cross-functional teams around the world, including a friendly "Security Feud" competition to win TikTok swag for claiming the top score on a range of cybersecurity topics.

We believe our ability to protect against threats is only as strong as our ability to identify and work together to address them. This fall, we hosted a global security leaders offsite, featuring guest speakers and a "field trip" to IBM's Cyber Range where our team was tested with a simulation requiring them to come together to manage seven crises simultaneously. We know it's not enough to build security into our product. We also have to test our own defenses, both as a team and with outside partners who help us continually improve the safety and security of our platform.

> **"We don't rise to the level of our expectation; we fall to the level of our training"**

You'll be talking at next year's Ransomware Resilience Summit series on 'determining roles and responsibilities in a response'. How critical is it for the business to pre-determine their responses and responsibilities to an attack before it happens?

There are a handful of sayings that I often share with my team. One is that, "we don't rise to the level of our expectations; we fall to the level of our training." Or to quote Ben Franklin, "an ounce of prevention is worth a pound of cure." It's critically important to have a plan, along with a back up plan. We have an entire team focused on business resilience and crisis management at TikTok. Their job is to anticipate worst-case scenarios and then create strategies to mitigate them.

This team is part of TikTok's global Fusion Center operations, which are an important cornerstone to address the converged global threat landscape we face every day. These operations fuse critical business, security, legal, privacy, communications, and other cross-functional stakeholders to ensure alignment across all parts of the business. Our approach helps to provide a comprehensive view of how our business and community intersects with the world -- both on and off the platform. However, our mission is about more than protecting against malicious threats. It's also about ensuring the platform's availability and reliability for exciting global LIVE events like the Ultimate Super Bowl LV Pregame Experience, UFC Fight Night, TikTok UEFA EURO 2020 Show with Ed Sheeran, an innovative concert experience with The Weeknd, or an around-the-world museum tour to explore art and culture.

Our all-hands, all-hazards incident management approach focuses on four pillars:

1. Understanding our critical business operations, assets, services, and community
2. Enabling over-the-horizon threat monitoring capabilities to detect and defend threats to our business operations, assets, services, and community
3. Protecting against events that negatively impact our community and business on and off platform
4. Rapid response capabilities to minimize impact if something bad were to happen

We're also creating customized, threat-led defense technology and capabilities that combine industry-recognized frameworks like VERIS, MITRE ATT&CK, CSF, Data Defense, and ISO 27001. As the threat and cyber criminal landscape changes, so are we by building new protocols and systems to detect, manage, triage, and escalate all types of security events spanning ransomware, organized cyber crime, and inauthentic behavior. Our multidisciplinary approach enables us to catch and eliminate potential security and safety incidents or adversaries before they put our platform or community at risk.

What are you most looking forward to by being a part of the Ransomware Resilience Summit series?

It's critical for the business community to get together, educate, and connect with one another. Industry forums like the Ransomware Resilience Summit are important because they bring together key stakeholders -- from security practitioners to law enforcement officials -- to share lessons learned and enable stronger defenses. The ability to connect digitally and in real-time is not just important, but maybe the most important driver of economic opportunity and change in our lifetime. The more we can learn from and uplift one another, the safer and more secure our world will be. I look forward to sharing the stage with fellow practitioners next year and continuing these important conversations.

With Cyber Security Awareness month behind us, what do you have planned for the #BeCyberSmart campaign moving forward?

Cybersecurity Awareness Month may be over, but we aim to encourage online safety year round. For International Fraud Awareness Week (November 14 - 20), we're joining the Association of Certified Fraud Examiners (ACFE) as a continuation of our #BeCyberSmart campaign. We're hosting a special #LearnOnTikTok LIVE stream on November 15 in conversation with @Alex_Falcone and industry experts sharing tips on how to avoid falling victim to fraud, because fraud is not a victimless crime. In the physical world, we follow expert guidance: "If you see something, say something." The same principle applies to the digital world, and people with cybersecurity skills have the power to protect those around them by sharing their expertise. We're welcoming security practitioners and companies across all industries to join us in creating TikTok videos to help others #BeCyberSmart.

Roland will be speaking alongside 30+ other experts at the upcoming Ransomware Resilience Summit series (London, February 22-23 and Washington D.C., March 29-30). Limited places are available to join TikTok, Netflix, Bupa, Microsoft, Oracle, Aston Martin, Trainline and many more behind closed doors and share best practices and lessons learned for tackling the unabating ransomware threat.