RSAConference2021

May 17 – 20 | Virtual Experience

RESILIENCE

THE TRENDS OF 2021

REFLECTIONS FROM RSAC 2021 SUBMISSION REVIEWS

EXPLORE THE TRENDS

CO-AUTHORED BY:

BRITTA GLADE
Senior Director,
Content & Curation
RSA Conference

KACY ZURKUS
Content Strategist
RSA Conference

RSAC 2021

The experiences and changes brought on by the pandemic have impacted all of us. Speaker submissions for RSA Conference 2021 reflected internalization of trials and challenges, rapid pivots to protect and enable businesses, and blossoming innovation in the face of significant hurdles. Lessons learned and experience gained in a year of resilience have forever changed us. When we selected our 2021 theme of ***Resilience*** long ago, little did we know how deeply appropriate it would be.

Each year, industry leaders from around the globe submit applications to speak at RSA Conference. In our pool of nearly 2,000 submissions, we saw a lot of evidence that cybersecurity professionals are looking to improve from both a functional and technical standpoint, but we also noted that this year's submitters were looking to inspire those who don't fit the typical mold of a cybersecurity professional. As you might imagine, narrowing the trends down was a bit challenging, so we solicited the help of our Program Committee (PC). Here is a look at five trends that our PC Members identified in their tracks, as well as five tracks that were created as a result of the RSAC 2021 submissions

CLICK BELOW TO SEE WHAT THE FUTURE HOLDS FOR OUR INDUSTRY.

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

EVOLUTION OF ROLES

As we've seen every year, there were many submissions that spoke to the evolution of the CISO, who is increasingly required to have more frequent communication with the board; thus, attendees at RSA Conference 2021 will have the opportunity to learn about the ways that CISOs can develop new communications skills. We are seeing a trend in the rise of Chief Product Security Officers (CPSOs), a role PC member Megan Samford on the Securing All the Things track pointed out is separate from a CISO. The CPSO, "covers the security of what a company sells—building security in, both in terms of features and secure development, throughout the lifecycle of a product."

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES | STRAIGHT TALK ABOUT ML & AI | INFORMATION MANIPULATION AND ITS IMPACT | RANSOMWARE ATTACKS | SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES | SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY | ZERO TRUST... WITH WHISPERS OF SASE EMERGING | ALL HAIL THE CLOUD | PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

STRAIGHT TALK ABOUT MACHINE LEARNING & ARTIFICIAL INTELLIEGENCE

This year's PC for the ML & AI track was pleased to see talks that focused on the practical realities of using AI and ML. "These are vast, confusing technical areas, and in previous years we saw a lot of "magic unicorn glitter"—which made this year's submissions a welcome change," wrote Diana Kelley and Saurabh Shintre. "The trend this year was towards lessons learned, applicable takeaways for organizations and practitioners as well as limitations and issues around potential harms of AI." Kelley and Shintre really appreciate seeing more practical use cases in submissions offering ways to generate and catch spam using AI tools like Generative Pre-trained Transformer 3 (GPT-3), how ML can inject fairness into federated learning, how to stop attacks on advanced driving-assistance systems, and how ML is in use today at large financial services institutions to advance data visualization and automation to combat fraud.

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

INFORMATION MANIPULATION AND ITS IMPACT

A resounding theme this year is echoed in the title of one of this year's Human Element sessions: Invisible Security: Protecting Users with No Time to Spare. Trending more than phishing, though, was disinformation campaigns. Andrea Little Limbago, PC member on the Human Element track, wrote,"There were also several submissions on disinformation campaigns and their security impact. On the one hand, this is not surprising given the widespread impact of these campaigns from many of the same threat actors."

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

RANSOMWARE ATTACKS

Greg Day was not surprised to see a continued focus on ransomware in the Hackers & Threats track. “We have seen the attacks becoming more sophisticated and targeted. Often they are now carrying multiple payloads such as ransoming data access but also either reselling the data or extorting further funds under threat of posting non-public data in the public domain,” Day wrote. “And while some ransomware is still focused on random victims, others have become far more targeted. The healthcare industry has certainly seen the pain from this.”

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES
STRAIGHT TALK ABOUT ML & AI
INFORMATION MANIPULATION AND ITS IMPACT
RANSOMWARE ATTACKS
SHARE AND SHARE ALIKE
RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES
SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY
ZERO TRUST... WITH WHISPERS OF SASE EMERGING
ALL HAIL THE CLOUD
PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

SHARE AND SHARE ALIKE

Submissions reviewed by the Analytics, Intelligence & Response PC revealed that more intelligence sharing is needed. Todd Inskeep wrote, “Several organizations have learned lessons that work in specific sectors (like the Cyber Threat Alliance for the cybersecurity industry) and plan to share lessons on how to make sharing work better and make it more valuable. Perhaps the most intriguing thesis is that aligning intelligence sharing to business needs can drive more valuable sharing of insights.”

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

Resilience, which is core to our industry and is key to define clearly, was highlighted more and more in submissions as discussions shift to calibration of risk; indeed, our Risk Management & Governance track is full of actionable approaches. The challenge of the rapid flip to a predominantly dispersed workforce was significant enough that we decided to highlight it in the new Securing the Remote Workforce track, designed to provide prescriptive guidance to threats from a home-based workforce and recommendations for organizations needing to adjust to the normalization of changes that have been implemented. The track will also look into the future and deliver concrete ideas to help organizations thrive in a sea of change. Assessments have shined the light on challenges and opportunities for organizations that have quickly pivoted, and continuous controls monitoring is being used to help companies raise the bar and evolve cybersecurity resilience. Threat hunting was a significant "micro trend" within this macro trend of resilience, with submissions focused on proactive approaches and picking up on untraditional and difficult-to-find threat indicators like lateral movement, exfiltration, compromised accounts, C2 activity detection, impossible journeys, internal recon, abnormal processes and many more nuanced activities as they worked to scan themselves in search of problems. The significant uptick on "art of the hunt" submissions was of great interest, as was the employment of artificial intelligence to enhance the work of human hunters.

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES | STRAIGHT TALK ABOUT ML & AI | INFORMATION MANIPULATION AND ITS IMPACT | RANSOMWARE ATTACKS | SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES | SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY | ZERO TRUST... WITH WHISPERS OF SASE EMERGING | ALL HAIL THE CLOUD | PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

Another trend within the macro trend of resilience that bears its own review is supply chain security and, related, software integrity, particularly in light of the SolarWinds breach and the ever-growing list of related breaches, a theme that will be touched on in many keynote and track sessions. The 2021 submissions explored the implications of our supply chains on third-party risk, physical security, operational security and business continuity, and also examined the very real and growing geopolitical tensions on supply chain resilience. Always seeking actionable guidance in the material put forward for RSA Conference attendees, the Program Committee was pleased to see sessions focused on the Digital Bill of Materials (DBoM) and Software Bill of Materials (SBoM) as tools to help address supply chain risk management challenges and public-private collaboration opportunities. Reliability, code integrity and good development practices as a theme within DevSecOps & Software Security submissions was also at an all-time high in the proposals reviewed, pointing to steps in our community toward more secure application development processes.

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES
STRAIGHT TALK ABOUT ML & AI
SHARE AND SHARE ALIKE
INFORMATION MANIPULATION AND ITS IMPACT
RANSOMWARE ATTACKS
RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES
SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY
ZERO TRUST... WITH WHISPERS OF SASE EMERGING
ALL HAIL THE CLOUD
PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

Zero Trust, likely assisted by the overnight remote workforce, rocketed up the adoption curve. We've started to see a healthy bank of submissions from end-user organizations willing to share explicit, direct experiences and recommendations coupled with guidance on controls and technologies needed to help overcome roadblocks to implementation and ease the steep learning curve. Submissions have matured to explorations of security capabilities, debates about the pros and cons of standardizing interfaces (i.e., APIs) for integrating different vendor products, potential architectural challenges and opportunities, and actionable guidance for companies looking to secure access for workers, workloads and the Enterprise of Things. SASE, however, seems to be where CASB was a few years ago, ascending the vendor hype cycle, though we would anticipate seeing rapid changes here.

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

ALL HAIL THE CLOUD

Related, but worth its own call out, is the explosion of high-quality cloud security-related submissions. Sessions explored the challenges and opportunities of remote management and delivery of … everything. "Everything as a Service" themes, supported by a cloud infrastructure, permeated submissions—endpoint, identity, network, email and security operations centers, as ways to protect sensitive information, were examined. Submissions also explored the impact of primarily cloud-based deployments on timely dissemination of threat intelligence to all vectors of compromise, which are no longer deployed in centralized locations. On the application security front, we also observed submissions around purpose-built cloud applications that required security in the apps, and on the other end, more adoption of cloud services, with the expectation of app security built-in. The far-reaching impact of this rapid move to the cloud will arguably be felt for years, presenting—perhaps—an opportunity for security to no longer introduce friction into the system and rather help reduce friction in the system. Indeed, there seems to be a significant opportunity here for developers.

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES
STRAIGHT TALK ABOUT ML & AI
INFORMATION MANIPULATION AND ITS IMPACT
RANSOMWARE ATTACKS
SHARE AND SHARE ALIKE
RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES
SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY
ZERO TRUST... WITH WHISPERS OF SASE EMERGING
ALL HAIL THE CLOUD
PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

The changing nature of the privacy conversation, which we did touch on in last year's trends, continues to evolve. Whereas in the early years our Privacy track was fairly narrow and of interest exclusively to privacy practitioners, this year the overlap of selections of "privacy-minded" sessions within other tracks was profound, and mature privacy-focused frameworks and codification of processes have emerged that will further drive privacy into corporate architecture and operations. Very clearly, privacy is a cornerstone to the cybersecurity ecosystem, seeming to move to a core value vs. a compliance checkbox for many, though unintended consequences are emerging and the hackers are taking note. The tone of privacy-related submissions also changed. Last year CCPA seemed positioned to take over the federal scene and radically disrupt industry but seemed to lose some steam when COVID-19 hit, and the tenuous balance between privacy and security lay raw, exemplified very clearly in contract tracing challenges and other risks related to identity tracking. New legislation in the area of data protection, privacy and security has also emerged, and the California Privacy Rights Act (CPRA) with its GDPR-like reach in California will likely change the way we're regulating ourselves in upcoming years. And, as with every other area of our lives and industry, COVID-19 has likely forever impacted the relationship between privacy and security, and clear lessons have been learned.

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST… WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS

RSAC 2021

Coming back full circle to where we started: We are a resilient industry comprised of resilient humans. No part of our worlds, small or large, personal or professional, was left untouched by the events of the past year. We look forward to sharing education and experience, learnings and challenges, as we come together as a community at RSA Conference 2021.

LEARN MORE ABOUT RSAC 2021 >>

<< RETURN TO INTRODUCTION

EVOLUTION OF ROLES

STRAIGHT TALK ABOUT ML & AI

INFORMATION MANIPULATION AND ITS IMPACT

RANSOMWARE ATTACKS

SHARE AND SHARE ALIKE

RESILIENCE OF PEOPLE, PROCESSES AND TECHNOLOGIES

SUPPLY CHAIN SECURITY & SOFTWARE INTEGRITY

ZERO TRUST... WITH WHISPERS OF SASE EMERGING

ALL HAIL THE CLOUD

PRIVACY FURTHER ENTRENCHED INTO ARCHITECTURE & OPERATIONS