RSAConference2020

San Francisco | February 24 – 28 | Moscone Center

HUMAN
ELEMENT

THE RSAC 2020 TREND REPORT

WHAT YOU CAN LEARN ABOUT THE FUTURE OF CYBERSECURITY

EXPLORE THE TRENDS >>

CO-AUTHORED BY:

BRITTA GLADE
Director, Content and Curation,
RSA Conference

KACY ZURKUS
Content Strategist,
RSA Conference

RSAC 2020

Each year, industry leaders from around the world submit an application to be a speaker at RSA Conference. This year, we received 2,400 responses to our 2020 Call for Speakers.

By sifting through all the entries, we were able to identify 10 trends that weaved their way through many of the submissions. Examining these trends provides a glimpse of what will be on the minds of cybersecurity professionals in 2020, and possibly beyond.

Click below to see what the future holds for our industry.

EXPLORE THE TRENDS >>

HUMAN ELEMENT

SECURE PRODUCTS

IT AND OT SECURITY

SECURE ENGINEERING

PRIVACY

THREAT INTELLIGENCE

FRAMEWORKS

SECURITY AWARENESS

COMMUNICATION

PROFESSIONAL DEVELOPMENT

HUMAN ELEMENT

When actress, writer and producer Tina Fey took the stage of RSAC 2019, she initially confessed that she saw very little—if any—overlap between her industry and cybersecurity. As Hugh Thompson, RSA Conference Chair probed, though, it became clear that there is something universal about human behavior that transcends time, generation and industry. Perhaps it was this very conversation that solidified this year's theme, Human Element.

Of the nearly 2,400 submissions, we saw "Human Element" embraced across sectors and silos, with challenges and successes of human behavior intertwined within discussions of data, threats, risk, privacy, management and teams. An overwhelming number of submissions started with a focus on human impact as a means of offering insight on how to better leverage common frameworks, inform decision makers in risk management, mitigate new and emerging threats and build a productive security-centric culture. Submissions explored the use of software and platforms to exploit humans—intentionally and unintentionally—reflecting on privacy implications as well as potential opportunities to use machine learning (in a continued evolution of the man/machine relationship we've explored in these submission trends reviews over the years). The broad stroke of the human element brush also looked to take on some elephants in the room that can hinder the success of the overall security program. This year's theme seemed to give submitters license to tackle the more sensitive challenges of human behavior, such as the potential downfall of toxic working environments, both to individuals and teams, and the risks to the security program that can stem from cybersecurity and engineering failing to leave their egos at the door.

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

DESIGNING, DEVELOPING AND MAINTAINING SECURE PRODUCTS

The 2020 submissions saw more deep dive technical submissions focused on secure product development than ever before, so much so that we have added new focused tracks on Product Security and Open Source Tools. Sessions explored UX design, from the standpoint of identity, artificial intelligence, privacy and SOCs; you name it, submitters homed in on how to make sure products were secure across the ever-expanding and connecting supply chain. Insightful proposals from developers across geographies and verticals aimed to help others learn from and through successes and failures on issues such as secure development lifecycles and frameworks, securing connected products and services, maintaining secure open source code andthe rising need for official CPSOs (Chief Product Security Officers). Many of the submissions also recognized the challenges organizations are grappling with in how best to use, maintain, test and certify the security of open source code, putting forth best practice considerations. If there's one thing that's a constant, it's that this industry does care about and support each other, and the wide array of talks proposed speak to the overwhelming desire people have to help each other, and subsequently lift the overall security posture of us all.

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

CONVERGENCE OF IT AND OT SECURITY

As the physical and cybersecurity worlds continue to converge, the roles and responsibilities of the security function are evolving. We are seeing more Chief Security Officers (CSOs), with responsibilities spanning physical and logical security, and increasing conversations around industrial control systems, thanks in part to NotPetya, the gift that keeps on giving. One of the challenges with IT/OT convergence is that these are two *very* different cultures and supply chains; thus, the convergence is also driving cultural changes in order to address the need for greater collaboration. We would expect to see frameworks pop up to help operationalize this convergence of security responsibilities (more on frameworks below). Convergence extends beyond ICS, though, which we believe contributed to the upward trend of 5G in this year's submissions. We additionally saw a continued uptick of proposals on smart homes and smart cities, with looming concerns about supply chain risks and how to ensure critical networks will function in a crisis.

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

A FOCUS ON SECURE ENGINEERING PROCESSES

In a related trend, we observed continued growth and maturation in DevSecOps-centered proposals as developers and security teams continue to work to define security's place in the DevSecOps world and the requirements needed to build capabilities and ensure the security of those capabilities. Risk management, and governance and compliance factors were explored in the context of DevSecOps as two traditionally "unrelated" audiences have suddenly found themselves working together productively, another positive nod to achieving secure products with integrated communication, processes and frameworks across organizations. Between shifting left and shifting center, there's a lot of moving and shaking going on in the world of DevSecOps. In another nod to the theme, learning how to find, hire and nurture the right individuals and teams for development was also a key theme in submissions, as experts detailed through actionable case studies how best to align with, integrate with and support other functions within organizations utilizing frameworks, dashboards and good old-fashioned human-to-human communication. We also saw some very thoughtful use case-centered submissions looking at when DevSecOps just doesn't make sense for an organization (that infusion of "risk management" assessment being put to the task).

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

INTERTWINING OF COMPLIANCE AND PRIVACY … AND PRIVACY AND EVERYTHING

A logical by-product of GDPR, this year's submissions indicated that there seems to be an operationalization of privacy with concerted efforts around frameworks and—consequently—automation. There was a notable shift in the tone and type of privacy-related submissions, reflecting of some maturation and understanding of the impact of privacy across products, services and organizations. That maturity seemed to also be a driver for more technical submissions, including homomorphic encryption. Where privacy once was a nice-to-have indication of "good corporate citizenship," it seems to now be trending as a core business and security conversation as organizations look to capture and protect user intent, not just because of regulatory compliance concerns, but also to provide business differentiation and positive user experience. We see the "privacy" and "security" functions within organizations working together in new, positive ways. RSAC 2020 sees us squarely in a world that is heavily in flux with privacy conversations, and this year's submissions highlighted challenges and unintended consequences of GDPR, a rapidly exploding landscape of regional, national and global privacy regulations (some in conflict with one another), exploration of ethical considerations related to privacy and data security and an overall sentiment of "we can and must do more, better."

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

THREAT INTELLIGENCE AND SHARING

Based on the submissions received this year, it's clear that security professionals see the value in building a Collective Cyber Defense and public-private collaboration. This has been an interesting pendulum-swinging exercise to watch (as explored in past trends write-ups), and this year we appear to have once again arrived at the value of sharing intelligence, perhaps due to further confidence in technical frameworks and mechanisms to do so. With the growing focus on fraud and identity, we saw more submissions related to user behavior analytics, indicating a strong link between behavioral sciences and cyberthreats. Playing into the human element, many submitters pointed to the power of threat intelligence and sharing while recognizing the continuous need to upskill security teams. As AI continues to spread its wings, we also saw an uptick in automation, for good and bad. Set against the backdrop of the 2020 US presidential elections and rising geopolitical concerns, classic social engineering meets the scale of automation was documented, with attackers leveraging machine learning and submitters exploring viable defenses against this growing challenge. Threat intelligence relies on trust, and though AI has the potential to inform, there must be a balance between automation and humans. With the maturation of this space and, indeed, the infusion of artificial intelligence and machine learning into just about every process across organizations, we saw an increase in submissions that documented the inherent weaknesses and challenges of machines, with some deeply technical and wonderfully detailed submissions digging into the specifics and providing guidance and best practice considerations.

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

FRAMEWORKS, AND FRAMEWORKS UPON FRAMEWORKS

In what is likely an indication that there is an ongoing formalization of processes, cross-departmental efforts between divisions within organizations and across organizations, and a drive toward automation, many of the 2020 submitters wanted to dig deeper into frameworks. These submissions looked at both hard and soft skills. We saw a rich number of submissions related to the MITRE ATT&CK framework, the NIST Cybersecurity Framework, Competing Security Culture Framework (CSCF) and the Factor Analysis of Information Risk (FAIR) Framework. Privacy frameworks also burst on the scene with a healthy number of submissions. The continued development and application of these frameworks—and the further mushrooming and morphing of more each year—appears to be driven by a desire for more efficient governance and improved risk management. Yes, risk management is the thread that binds all of these trends in some way, shape or form.

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

SECURITY AWARENESS AND TRAINING

Given the overarching theme of RSAC 2020, it's no surprise that we saw security awareness and training topics trending in this year's submissions. While some Program Committee members initially saw security and awareness training as a part of the Human Element track, it became clear that threats don't discriminate. As our world becomes more interconnected and we rely more on connected devices and artificial intelligence to inform decisions, it is equally as critical that we break down the siloed approach to awareness and training. Recognizing the value of training, many submissions included the term "Cyber Range" and touted the value ranges bring to developing and honing skills. Some submissions addressed the moral and ethical issues of security awareness, while several highlighted the need for more attention on workplace stress and mental health, particularly for security practitioners. Evidenced in the word cloud with learn, team, talk, discuss, help and understand, this year's submitters really internalized what it means to be human, thinking more deeply about how individuals interact with each other and what teams need in order to collaborate efficiently and effectively.

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

COMMUNICATION

Many of this year's submissions highlighted the human need for clear communication. In order to do their jobs effectively, CSOs need to understand all that has moved into the realm of their purview. To that end, we saw several talks that offered guidance on how to prepare CSOs for all aspects of the job. This collection of submissions offered a variety of ways to help CSOs and CISOs where they need it most: communication up, down, across and throughout their organizations and the organizations that are part of their extensive supply chains. We received submissions on everything from creating a good cybersecurity dashboard for the board to how to use metrics in order to create successful presentations to how to help different functions within organizations to *really* talk to and understand each other, not just in words but in actions (the rise of purple teaming is achieving great things for organizations).

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

PROFESSIONAL AND WORKFORCE DEVELOPMENT

Increasingly, enterprises are trying to fill the growing skills gap, searching for diverse candidates to fill many different roles. Recognizing the need to attract and keep talent, the very definition of diversity has expanded beyond the confines of gender to include not only race, age and ethnicity but also the diverse workings of the human mind. This year's submissions reflected that people clearly internalized the question of what it means to be *human* in how we learn, communicate and interact with each other and with technology. Submitters were clearly thinking from a security mindset about what individuals need to do their jobs as well as what team members need to interact with each other more productively. Additionally, proposals raised the question of how to hire, train, retain and inspire talent.

READ THE CONCLUSION >>

<< RETURN TO INTRODUCTION

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT

RSAC 2020

These 10 trends just scratch the surface of the breadth and depth of the body of knowledge and experience that flowed through this year’s submissions. Other key words such as zero trust and serverless, Kubernetes, quantum, chaos engineering, bug bounties and endpoint decay (or resurgence, depending on who you ask!) abounded; we are a passionate community with diverse and rich expertise that wants to connect, share, protect and defend.

Our opportunities—and responsibilities—are very real. As measured by the World Economic Forum’s 2019 report, two of the top five likely risks to the world—right behind extreme weather events, failure of climate change mitigation and adaptation, and natural disasters—lie squarely in our purview: data fraud or theft and cyberattacks. On this tightly connected, highly interdependent supply chain that is Planet Earth, the threats and potential for impact are very real, and now, more than ever before, there is a need for the humans among us to gather, share, build, and work cooperatively and productively together. We look forward to seeing you in San Francisco at RSA Conference 2020.

LEARN MORE ABOUT RSAC 2020 >>

HUMAN ELEMENT | SECURE PRODUCTS | IT AND OT SECURITY | SECURE ENGINEERING | PRIVACY | THREAT INTELLIGENCE | FRAMEWORKS | SECURITY AWARENESS | COMMUNICATION | PROFESSIONAL DEVELOPMENT