FORRESTER®

# Predictions 2021: Cybersecurity

October 26th, 2020 | Jeff Pollard, Heidi Shey, Joseph Blankenship, Jinan Budge, Paul McKay with Amy DeMartine, Melissa Bongarzone, Ian McPherson

## At A Glance

- Pandemic-related uncertainty, remote work conditions, and employee experience (EX) collide to create the ideal conditions for insider incidents. One-third of security breaches will be caused by insider threats in the coming year. Security and risk professionals must adapt to this new reality.
- The US grip on control of the cybersecurity startup scene will erode further, with investment activity exploding in Europe and Asia Pacific in response to rising geopolitical tensions.
- Consumer buying patterns will force brands into direct-to-consumer models, which will also increase security breaches as marketplaces and digital experience initiatives leave companies exposed. For more information on our predictions for cybersecurity in 2021, please schedule an inquiry.

## In 2021, S&R Pros Must Address Issues Of Insiders, Team Culture, And Geopolitics

Personally and professionally, 2020 was not the year security and risk pros wanted or expected. But it is a year that taught us what we could endure. 2021 will not see things return to normal — yet — but it will be the beginning of the transition back to normal. This will simultaneously require us to adapt while remaining resilient. Forrester predicts that in 2021 security and risk pros will experience:

- **Thirty-three percent of data breaches will be caused by insider incidents, up from 25% today.** Insider incidents may be caused by accidental or inadvertent data misuse or due to malicious intent. In 2019, Forrester security survey respondents indicated that 25% of data breaches were caused by internal incidents of this nature. The rapid push of users to remote work during the COVID-19 pandemic, fear of job loss, and the ease with which data can be moved will lead to an increase of insider incidents from 25% today to 33% in 2021. As firms add capabilities for detecting insider threats, they will also be able to identify and attribute more incidents to insider activity than they were previously. Give specific focus to insider threat defense, emphasize

employee experience to avoid turning employees into malicious insiders, and remember that trust is not a control.

- **Funding for non-US headquartered cybersecurity companies will increase by 20%.** VC funding for cybersecurity firms globally reached dizzying heights before the COVID-19 pandemic hit, as firms raised $11.7 billion in 2019, with only $4.3 billion raised outside of the US. While funding has dipped this year due to the pandemic, Forrester expects funding for non-US cybersecurity firms to increase by 20% in 2021 over its 2019 baseline. Moves by the EU commission to promote its digital sovereignty and further economic protectionism especially in Asia will result in increased funding for regional cybersecurity firms. For multinational companies, S&R pros must give up their single sourcing approach and accept the reality of point solutions based on region. CISOs should develop a startup scouting capability to identify promising new regional security technology, build an adaptable procurement and sourcing plan to obtain them, and create standard security guidelines to create consistency across disparate vendors.
- **A CISO from a Global 500 firm will be fired for instilling a toxic security culture.** Empowered employees understand that social media can amplify concerns if their company disregards them. Professional networks once privately shared details of toxic leaders and individuals to avoid, but now that conversation will become public — rightfully so. AMP shareholders pressured the firing of a trio of executives for harassment claims, and the Ellen show snagged the spotlight for bullying issues, with three producers ousted as a result. Expect such repercussions to hit CISOs, given the rise in visibility of the role. Leaders that create, tolerate, or ignore hostile cultures are on notice that 2021 will be a year of reckoning. Eight of Forrester's top 10 causes for toxicity in cybersecurity relate to a failure in leadership. Cultivate a positive culture for your team to thrive in, and invest in the hard work to teach the soft skills of empathy, vulnerability, and people management.
- **Retail and manufacturing will have more breaches due to direct-to-consumer shift.** As consumer buying habits undergo a massive paradigm shift, brands that once went to market via retailers and distributor supply chains face disruption, forcing them to now sell directly to consumers. While a direct-to-consumer shift was already under way before COVID-19, the pandemic accelerated the timeline. Today, 44% of US online adults get tired of going to several stores to research or buy product, while conversely, 62% had performed an online transaction. This shift requires companies to expand their attack surface by adding digital storefronts and marketplaces and adopting new engagement models. More customer-facing applications means more code, and more code means more risk. In 2019, 40% of global enterprise security decision makers said a breach happened by exploiting a software vulnerability, and 37% said it was through a web application. If your firm is shifting to direct-to-consumer, prioritize product security, build a developer champions program, and explore breach and attack simulation tools.
- **Audit findings and budget pressure will lead to uptake of risk quantification tech.** Different regions and verticals have experienced vastly different effects due to COVID-19, but most companies face economic uncertainty with a prolonged recovery period. Firms struggling to survive will make harsh technology and people cuts, causing them to struggle to prove compliance. Firms

 

attempting to maintain the status quo will find themselves facing tough decisions too. In 2021, CISOs must prioritize what to do and where to invest to overcome audit issues, manage risks, and protect the enterprise. Stagnant or declining budgets will require solid justification for spending. Risk quantification solutions that provide specific insights into the criticality of assets and potential impact of an issue in real time with business context will help security leaders determine what stays, what goes, and where limited increases should go. Examine risk quantification solutions — and their substantial required dependencies — to move beyond the tried-and-true basic business case that was sufficient during the growth years.

 