Cyber Threats Don't Require Sensationalism

Claire Umeda, Vice President of Marketing, 4iQ

If it bleeds, it leads. As news media has evolved, this adage remains true. And it's no surprise – fearmongering has historically worked in drawing attention. In the cyberworld specifically, many vendors rely on this tactic, but so do cybercriminals.

Currently, bad actors are exploiting the uncertainty surrounding COVID-19 through phishing attacks and malicious websites. Simultaneously, national outlets are sounding the alarm about increased attacks and vulnerabilities. There is reason for alarm, of course – our sense of normalcy has shifted completely. However, during times like these, we must remind ourselves to practice compassion, remain level-headed, and avoid stoking hysteria, which only plays into the hands of bad actors.

Stressing the importance of cybersecurity without resorting to fear-based messaging is no small order. It's a very nuanced issue that requires balance. On one end of the spectrum, there's breach fatigue – a sort of learned helplessness – where people respond to cybersecurity vulnerabilities with apathy or numbness. And who can blame them? Major breaches are constantly making headlines. We're well aware of the increased sophistication among cybercriminals, nation state actors, and threat actor groups, especially around election season.

According to my firm's 2019 Identity Protection & Data Breach Survey, among the respondents who were victims of a breach and were offered identity protection services by the affected companies, more than half did not enroll. There are simple

steps people can take to mitigate their risk of cybercrime, but because of the constant fear-based messages thrown at them, people buy into the fact that their information and privacy are already compromised, which it very well may be, and don't take any action at all.

The problem with this mindset is one person's negligence can put a whole corporation and its network at risk, just like the coronavirus will continue to spread if people don't take precautions seriously. Consider how often accidental exposure occurs. According to a survey conducted by software company Egress, 83% of security professionals surveyed believe their employees have put sensitive customer, personal and business information at risk. Long story short, apathy is not the response we want.

On the other end of the spectrum, irrationality ensues. People are fearful and end up making rash decisions. As media coverage of COVID-19 continues to center around doom and gloom, uncoincidentally, we've seen a spike in phishing scams. Security firm Barracuda Networks reported a 667% spike, to be exact. Widespread discussion of COVID-19 is important because awareness is key. However, an unintended consequence of the nonstop coverage is a higher level of attacks – cybercriminals know people are vulnerable and will fall prey to seemingly obvious scams. When the recipient of a phishing attack is already in a state of panic, they won't be as vigilant of suspicious activity. People want to know as much information about the coronavirus as possible to protect themselves, and may not think twice about clicking on a malicious link or attachment.

From a business perspective, interestingly, a 2018 study conducted by Lepide found that "fear selling" in more than 60% of the prospects the firm surveyed "made people less likely to engage (or buy) from a vendor." While fear draws attention, it doesn't always register with its intended audience.

Chris Krebs, Director of the U.S. Cybersecurity and Infrastructure Security Agency, put it best: "Fear sells, but we have far too much to offer to just be looking for the next mark. We've got to be more straightforward, more measured, more reasonable in how we talk about [threats]."

We must improve the way we communicate – myself included. It is especially important right now, when budgets are constrained, and cybersecurity isn't always viewed as essential or a resource that will contribute to the company's bottom line.

So just how should we communicate? First and foremost, instead of publicly lambasting companies who don't have great cyber security postures, let's instead choose to applaud those who do – or at least, those who make a concerted effort to do so. Take the recent Zoom privacy issues. In the wake of mounting problems, the company swiftly responded, acted transparently, and, importantly, appeared sincere and genuine. The videoconferencing company acknowledged its errors, and even though there are still ongoing issues, the company is doing what it can to adapt with its spike in users.

Along these lines, it's time to stop victim-blaming. Often times, the affected company is not entirely at fault. Reacting with a measured response is important, just as Mr. Krebs said. Focus on informing, rather than fear-inducing. Given the spread of disinformation, it is important that we dispel news that is patently untrue, backing up all claims with credible sources, including in marketing materials for your company. In other words, stand out from the crowd without putting out false information.

Further, the world of cyber is a foreign concept to a majority of the population, so it is key to make these issues relatable. Simply put, an issue will resonate only if you are able to draw connections to the audience in a digestible

manner. When engaging with a non-expert, analogies are your friend, and avoid jargon. Finally, it's important to walk the walk, and not just talk the talk. If there's a problem, provide a realistic solution (that isn't just your product). Can you imagine if Dr. Anthony Fauci laid out the dangers of the coronavirus without addressing how we would approach and fix this problem?

We have reason for optimism – the world of cyber will continue to adapt and innovate, keeping pace with ever-evolving cyber threats. However, there is a fine line between informing the masses and spreading fear. In our line of work, a lot of the threats we deal with are inherently scary, so there's no need to further sensationalize the issues.

About the Author: *Claire Umeda is Vice President of Marketing at 4iQ, where she leads go-to-market strategies, product marketing, sales enablement and brand management. Prior to joining 4iQ, Claire has held senior and executive marketing and product positions for startups in the security, communications, data management and social gaming spaces.*