TOPICS: Corporate Governance, Risk Management

February 8, 2022

The New Online Risk Isn't Cyber—It's Chatter

By Andrea Bonime-Blanc and Vikram Sharma

The past decade has been filled with cautionary tales detailing cyber risk's journey from the public to the private sector. Unfortunately, this same scenario is playing out all over again in another part of our digital world.

Nearly 10 years ago, following the first global survey on managing cyber risk, *Forbes* published an article titled "Boards Are Still Clueless About Cybersecurity." Since then, board-level conversations about cybersecurity have matured, and cyber risk's impact on corporate reputation and customer experience has become undeniable.

But now, a new risk has emerged. The actors and scenery may be different, but the story follows the same plotline. It's digital chatter.

What is digital chatter?

Digital chatter comprises all the conversations happening among users online, whether on the surface or the deep web. It includes open, indexed and closed, and dark social media channels. It also includes forums and messaging apps. Several recent examples include the deliberate use of social

media influencers to attack COVID-19 vaccine providers, the online planning of an insurrection at the US Capitol, and the coordinated efforts by a subreddit to short squeeze stocks.

Companies are taking notice: A recent Crisp survey of more than 100 corporate leaders, most CEOs from companies with revenue over $1 billion, found that—similar to what happened with cybersecurity 10 years ago—61 percent report their boards and leadership teams are already pursuing new skills, capabilities, or resources to keep up with risks that originate from or become amplified online by digital chatter.

That's consistent with a recent analysis of 75 annual 10-K reports by Forrester Consulting, which found that 67 percent of companies named social media a top risk. That number is expected to rise and become consistent with the 97 percent that mentioned cybersecurity breaches as a top risk. In addition, the study found that social media commentary, whether true or false, can affect a brand's value, corporate reputation, and operational and financial performance.

The Forrester study analyzed the operational and financial consequences of not identifying digital chatter risks early enough or at all, defining these risks as a crisis event. In fact, this type of crisis event is happening with greater frequency. Companies often face several of these events per year, posing costs and losses valued between $100,000 and $10 million.

While the learning curve for understanding risks driven by digital chatter is decreasing, the speed and scale of digital chatter are quickly increasing.

Why is this acceleration in digital chatter happening?

Recent stories of misinformation—associated with global health, national elections, and financial markets—and weaponizing social media have caused us all to reevaluate the danger of online conversations. In fact, 77 percent of the CEOs in the Crisp survey agreed that more companies will be targeted by organized groups online or Internet-savvy actors intent on damaging their brand within the next 12 months.

Unlike cyber-threat actors, who must have deep expertise on the channels they attack to deliberately do harm, anyone with a mobile phone can harness the power of digital chatter to knowingly (or unknowingly) disrupt or alter the future of your organization. Currently, more than half the global population—4.48 billion people—actively use social media. The speed and scale of their reach is enormous.

The deep web is where actors and groups often hone their skills and coordinate to harm organizations at scale intentionally by using digital chatter. Much like cyber-threat actors, these adversaries

constantly develop new tradecraft and share tactics to evade detection, becoming more sophisticated by the day.

Who owns digital chatter in an organization?

When an incident happens involving digital chatter, immediate attention is required from leaders, including senior executives, regardless of the time of day or day of the week. An active, coordinated response is needed involving key functions such as communications, marketing, security, human resources, and legal.

But what about before such an incident occurs? The challenge for corporate boards is determining who exactly is responsible for handling the risks from digital chatter, including developing a plan for mitigation and incident response.

Just as the key actor groups behind damaging digital chatter can be elusive, determining who owns digital chatter in an organization can also be slippery.

Digital chatter can originate or amplify many types of risks, both those identified on a formal risk register and the unpredictable ones, which have become far more common. If business resiliency is defined as an organization's ability to deliver on its brand promise and vision no matter what the crisis, then it stands to reason that communications leaders should play a central role in leading this cross-functional effort.

According to a recent survey of 100 communications leaders, 84 percent say they are already taking on greater responsibility in identifying and mitigating risks. Historically, given their role of effectively disseminating information across an organization, many report working cross-functionally with risk, security, legal, and human resources teams to do so.

Much like cybersecurity, risk intelligence has become far more sophisticated, using artificial intelligence and machine learning trained by industry-leading experts. The new field is quickly distinguishing itself from legacy social media listening platforms, which provide brand or competitive intelligence, consumer marketing insights, or advertising campaign analytics but aren't purpose-built for risk. It's important for both management on the front lines of tackling these risks and boards exercising risk oversight to understand this distinction.

What questions should we ask?

If your board is unsure about how your company is approaching this challenge, ask the following three questions of your chief risk officer or risk management committee:

1. Is our company often late to know about risks originated or accelerated by digital chatter?

2. Is our company a potential target for organized groups online whose intent is to exploit digital chatter to harm our brand reputation, communities, people, or assets?
3. Does our company still rely on legacy social listening tools to identify and mitigate risks instead of a formal risk intelligence capability?

If you answer "yes" to any of these questions, it's time to formally audit your company's management of risks driven by digital chatter. Boards should demand their C-suite embrace the lessons learned from cyber risk so that they can adopt new resilience models that prioritize risk intelligence and reduce exposure to this new risk in the digital world.

Dr. Andrea Bonime-Blanc is founder and CEO of GEC Risk Advisory and serves on several boards, including that of the NACD New Jersey Chapter. Vikram Sharma is president of Crisp, the leading provider of corporate risk intelligence.

COMMENTS

READ RELATED CONTENT

Digital chatter Risk