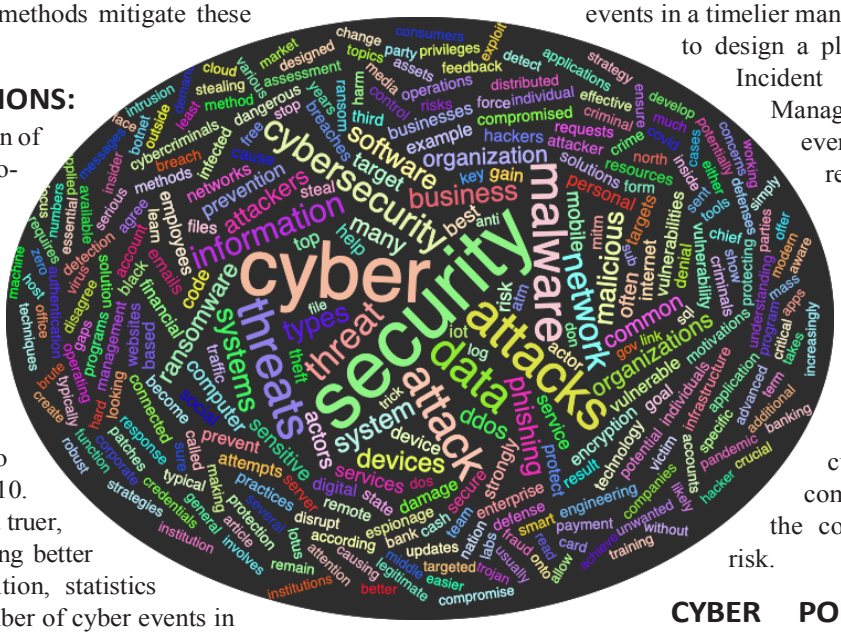
STATISTICAL SIGNIFICANCE

Long delays in reporting cyber events – due to a lack of information or to intentional suppression of information – negatively impacts an organization's ability to manage risk. Statisticians can provide those charged with managing cybersecurity with critical information related to cyber issues including system vulnerability, effectiveness of countermeasures, event trends, and improved forecasting. Statistics provides policymakers critical clarity into the opaqueness created by delayed reporting, allowing for more accurate estimations of the true exposure and risks associated with cyberattacks.

Cyber Industry

CYBER EVENTS: Cyber events can take months or even years to be detected and even more time to be reported. In addition, organizations are frequently reticent to report attacks because of brand damage and reputation impacts. As a result, any database with the most "up-to-date" information on cyberattacks is at best incomplete, but at worst biased and non-representative. Consequently, analysis conducted with such data would be incorrect and likely misleading. Statistical methods mitigate these issues.

COMPUTING CORRECTIONS: Statisticians use the distribution of reporting delays in recent up-to-date data to estimate the proportion of delayed (yet to be reported) cyber events at any given time. For example, if there are 10 known events, but statistical analysis suggests only 5% completeness, the actual event count would be closer to 200 rather than the known 10. The corrected counts provide a truer, more complete, picture enabling better informed decisions. In addition, statistics help predict the expected number of cyber events in the future using the corrected counts, providing more accurate representations of exposure and assets at risk.



UNDERSTANDING CYBER RISK: With corrected counts, statistics help in better understanding the current cyber risk landscape. Furthermore, statisticians create models that assist cyber insurers in quantifying risk. The creation of improved models—made possible by correcting for reporting delays—in turn provides insurers with better estimates of expected or possible losses and additionally helps them in determining how much reinsurance to purchase.

HOW CORRECTIONS HELP BUSINESSES: With a better understanding of the current cyber risk landscape, businesses can make more informed decisions, better assess the usefulness of their current cyber security measures, and determine where further efforts should be made. Cyber insurers also work with businesses to identify what countermeasures should be in place to prevent future cyberattacks, what measures could be taken to detect events in a timelier manner, and inform them to design a plan of action (Cyber Incident Response Management) should the event occur. These responses have the potential to save businesses millions, strengthen their reputation for maintaining strong cyber security, protect the personal data of their customers, improve compliance, and reduce the cost of exposure and risk.

CYBER POLICY MAKING: Developing a 360-degree view of cyber events is critical to informing cyber policies. This view needs to include answers to questions such as – What is the current rate of events? What kind of events are more prevalent in any given domain? How could cyber events impact a business or industry? Is there a certain type of event that has more impact than others? If yes, what measures could be taken to avoid them? Statisticians empower policy makers with more complete information. In addition, statistics inform expectations by forecasting cyber event rates, trends, and patterns in cyber events, as well as quantifying which policies have been effective in the past and which have not.