THE COST OF (NO) QUANTIFICATION

By 2021, cybercrime is likely to cost the world **$6 trillion** annually.

DO THESE QUESTIONS KEEP YOU UP AT NIGHT?

1. Are we spending our cybersecurity budget on the right things? What is the ROI?
2. Do we have enough cyber insurance?
3. How much risk do we have? Are we spending too much or too little?
4. We don't want to be the next news headline cybercrime victims. Are we doing enough to minimize risk?

HOW DO YOU ADEQUATELY ANSWER THESE QUESTIONS?

Leveraging quantitative modeling — known as cyber risk quantification (CRQ) — empowers your organization to fully understand the risks it faces **in business terms**.

WHAT'S THE VALUE-ADD OF CYBER RISK QUANTIFICATION?

Organizations **WITH** Quantitative Modeling		Organizations **WITHOUT** Quantitative Modeling
50%	Discover incidents in an average of less than one day	23%
66%	Less than 10 percent chance of suffering more than $1 million in cyberattack losses next year	35%
42%	Five or fewer critical open security vulnerabilities in customer-facing products	21%
62%	10 or fewer data loss prevention incidents last year	33%

Cyber risk quantification uses industry leading and highly vetted probabilistic models to more accurately describe the cybersecurity and technology-based risks facing an organization. Companies are increasing their use of quantitative risk methods because they work. Protiviti has been quantifying cyber risk since the beginning — partnering with organizations on small scoped engagements, full program transformation and maintenance.

protiviti®
Face the Future with Confidence

Source: *https://www.protiviti.com/US-en/insights/cybersecurity-imperative*