SonMax Consultants Inc.
24 Manor Drive
Marlboro, NJ 07746
E: sales@sonmax.com
T: +1 732.591.1512
F: +1 732.591.5424
www.sonmax.com

SONMAX
CONSULTANTS INC.

Why do companies play Russian roulette with their money?

Everyone talks about the costs of cyber crime and organizations agonize over spending thousands or hundreds of thousands of dollars/euros/pounds to develop effective preemptive strategies. Too often, companies prefer to leave their core assets at risk and fervently hope that they escape.

The reasons for this attitude are many:

- The costs associated with developing robust controls and protections are viewed as being pure cost and taking away from the bottom-line revenues of the company
- Companies simply do not have a good grasp on the real financial impact of cyber crime and thus under-protect, thinking that they're well protected. A great example is the unwillingness to write cyber crime insurance policies for larger organizations for more than say, $5 or 10 million.
- Those responsible for protecting organizations are hesitant to be the bearer of bad news; or be accused of crying wolf

Sadly, the truth is that too many companies engage in an "ostrich" mindset. If they don't see it, it won't happen.

So, what are the facts? Here is some public record information from just the last 4 weeks.

Cyber crime is the crime that keeps on taking:

- Target’s 2013 breach is ***STILL*** costing Target money
    - Target reached an $18.5 MM settlement with 46 states in mid-June 2017
    - To date, Target’s costs **exceed** $300 MM
    - It is unknown if they’re done yet

- Reckitt Benckiser announced the ***initial*** cost estimates from their June 2017 Wanna Cry Ransomware attack
    - RB release states a 2% Q2 cost versus 2016 Q2 Revenues
    - That translates into ~$58.2 MM
    - These are estimates and will revise (upward) over time

Multiply these costs by the hundreds of companies who were impacted by Wanna Cry, Petya or other data breaches since the start of 2017 and then contrast that with the costs of implementing sophisticated proactive cyber protective solutions:

- A robust IR Plan typically costs less than $250 Thousand
- Testing an IR Plan usually costs less than $100 Thousand
- Implementing vital Windows security patches cost less than $150 Thousand (this assumes that all systems must be taken down to implement the patches and suggests a high-end estimate to the operational impact of short-term planned outages)
- Implementing secure NFC and Bluetooth for POS environments is less than $250 Thousand for all but the largest retails firms (this is the delta between secure NFC/Bluetooth and out-of-the-box NFC/Bluetooth)
- Implementing multi-factor authentication (MFA) and biometric-based security is approximately $400 per employee

In other words, it is possible to spend $1 - 2 MM on protective measures -- but even at $2 MM, it is a great deal less than $58 MM or 300 MM.

The nature of the internet is that companies must pay something due to cyber crime. Companies can pay a lower number up front or a higher number on the back-end, potentially for years.

Ultimately, it's your choice.