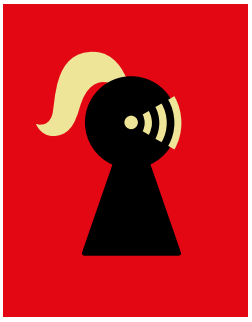
INTRODUCTION



Cyber threats are generating some scary statistics: $400 billion a year in losses from attacks, with some larger businesses experiencing more than 12,000 attacks each year. But there is also good news. Companies are recognizing that cybersecurity is not a technology concern but rather a critical business issue and one they are preparing to deal with. To address the significant business and reputational risks involved, companies are using a cross-functional, top-to-bottom approach, one that treats cybersecurity as a business imperative.

Many companies are beginning to strengthen their "human firewall," creating a business culture where every employee sees cybersecurity as their responsibility. People, not software, are often the weakest link in a security system and that is a problem no software patch will solve.

Regulation is growing increasingly complex and governments' expectations differ from those of companies and consumers. The rules are murky and lag far behind the technology – and the threat. To deal with competing and at times conflicting requirements, some companies are moving beyond the minimum demanded of them, and aiming for a higher standard.

To be effective, a company's cybersecurity program needs to weave these threads into its underlying business plan. Cybersecurity is more than just a strong defense, more than compliance. It must be a part of corporate culture. It represents an opportunity to differentiate yourself from your competitors, increase the efficiency of your operations and earn a greater level of trust from customers, shareholders and the community.

MARK SEIFERT, GEORGE LITTLE AND SIOBHAN GORMAN
Global Cybersecurity and Privacy practice, Brunswick Group

SOURCES: LLOYD'S, IBM / ILLUSTRATION: NOMA BAR