THE Cybersecurity STORM

MANY BREACHES HAPPEN BECAUSE BUSINESSES DON'T DOWNLOAD SECURITY PATCHES

85% of successful data breaches targeted the top 10 known vulnerabilities which have never been patched despite patches being available

83% of data breach victims took more than a week to detect a breach

Source: CompTIA, "Trends in Information Security," 2015

MOST CYBER ATTACKS ARE PERPETRATED BY INSIDERS

60% of cyber attacks in 2015

44.5% were considered "malicious"

Source: IBM: "2016 Cyber Security Intelligence Index"

THE GROWTH OF IOT IS HEIGHTENING THE SECURITY THREAT

70% of IoT devices are vulnerable to a security attack

Source: HP "Internet of Things State of the Union Study," 2014

EMPLOYEES NEED TO BE AWARE OF RISKS

Increasing employee awareness on cybersecurity practices will cause a

30% decrease to security risks

Source: "2015 Global Megatrends in Cybersecurity," Ponemon Institute LLC. (conducted for Raytheon)

SIMPLE, PREVENTABLE MISTAKES ACCOUNT FOR MANY SECURITY LAPSES

42% of individuals say end user failure to follow policies, or carelessness, were to blame

Source: CompTIA report

MANY ORGANIZATIONS AREN'T EFFECTIVELY PLANNING FOR INFORMATION SECURITY

43% of executives feel they have an effective information security strategy
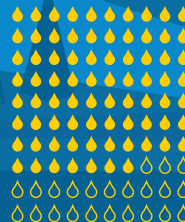
Source: PWC: "Cybersecurity: The new business priority," 2012

2/3rds of CIOs and CISOs said that their organizations don't see cybersecurity as a priority

Source: "2015 Global Megatrends in Cybersecurity," Ponemon Institute LLC. (conducted for Raytheon)

MANY SMBS UNDERESTIMATE THE CYBER THREAT

77% of SMBs say they believe their company is safe from cyber threats, yet…

83% have no formal security plan

Source: National Cyber Security Alliance (NCSA) and Symantec