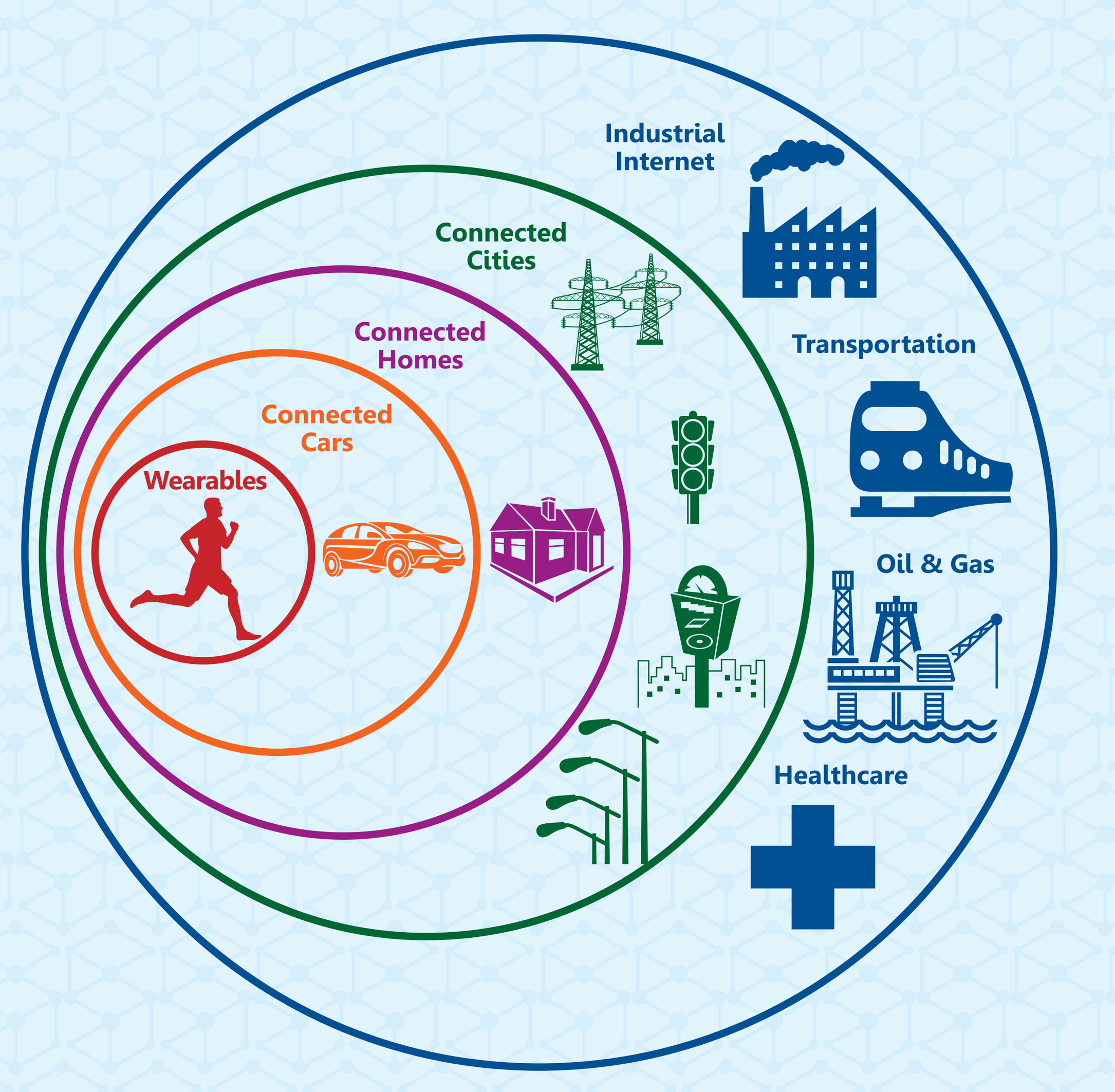
IoT LANDSCAPE

SENRIO
http://iot.security



Timeline of IoT

- '68 PLC is born — Dick Morley drafts basic design of a PLC. Theodore G Paraskevakos designs 'Machine-to-Machine' (M2M) concept
- '83 Ethernet standardized
- '86 PLCs are linked to PCs
- '89 World Wide Web — HTTP is first demonstrated by Tim Berners-Lee
- '92 Ethernet and Transmission Control Protocol / Internet Protocol (TCP/IP) — connectivity for PLCs is Introduced
- '97 Wireless M2M technology
- '99 "Internet of Things" — is coined by Kevin Ashton
- '02 Cloud Technology — takes hold with the launch of Amazon Web Services (AWS)
- '10 Sensors drop in price
- '16 IIoT vision emerges — includes 'Big Data', advanced analytics, and strong cloud integration

IoT Security

76% Considering strategies **IoT** Security Concerns

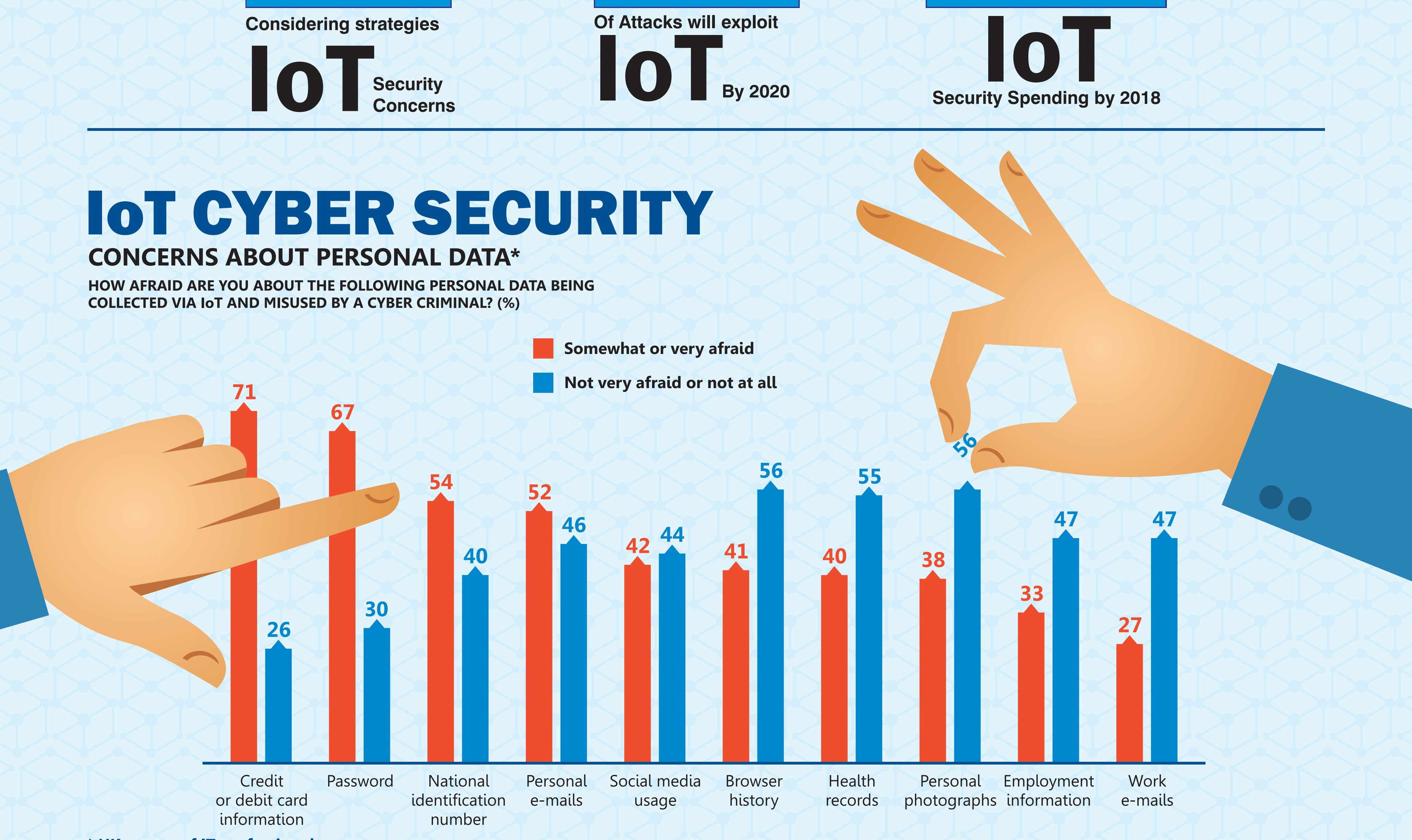
25% Of Attacks will exploit **IoT** By 2020

$550M **IoT** Security Spending by 2018

IoT CYBER SECURITY

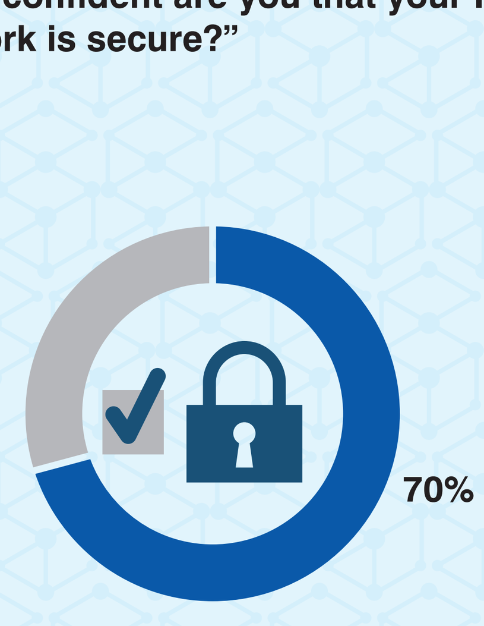
CONCERNS ABOUT PERSONAL DATA*

HOW AFRAID ARE YOU ABOUT THE FOLLOWING PERSONAL DATA BEING COLLECTED VIA IoT AND MISUSED BY A CYBER CRIMINAL? (%)



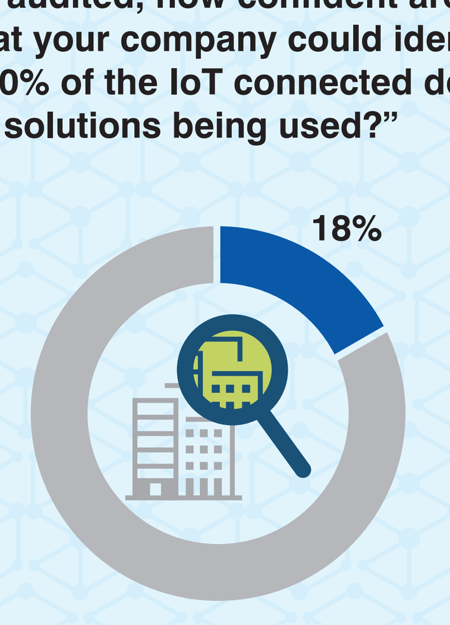
* UK survey of IT professionals

"How confident are you that your IoT network is secure?"



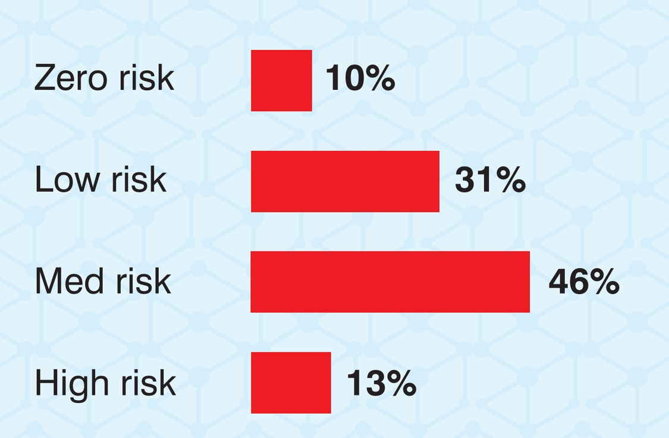
70% Highly confident

"If audited, how confident are you that your company could identify 100% of the IoT connected devices or solutions being used?"



18% Fully confident

"How much security risk is your company willing to tolerate in relation to compliance requirements for IoT security?"



Base: 603 IT and business decision makers with involvement in their organization's network and data security processes
Source: A commissioned study conducted by Forrester Consulting on behalf of ForeScout, August 2017

2017 IOT MALWARE ACTIVITY MORE THAN DOUBLED 2016 NUMBERS

The number of new malware samples in the wild this year targeting connected internet-of-things (IoT) devices has already more than doubled last year's total.

IoT devices at risk: malicious programs target the 'Internet of Things'

Currently, over 6 billion of 'smart' device exist globally. It was when the Mirai botnet emerged in 2016 that the whole world learned how dangerous such devices may become in the hand of cybercriminals. However, the history of malware attacking IoT devices began much earlier.

1. **HYDRA** — The first malware program targeting IoT devices. — 2008
2. **PSYBOT** — Emergence of Psybot, the first in-the-wild malicious programs for the MIPS platform. — 2009
3. **TSUNAMI** — A cross-platform IRC backdoor with DDoS Capabilities. — 2010
4. **GAFGYT** — An IRC backdoor capable of scanning IP ranges to find vulnerable devices. — 2014
5. **TROJAN. LINUX.PNSCAN** — A Trojan infecting vulnerable devices with the Tsunami backdoor. — 2015
6. **MIRAI** — and its clones Hajime, Remaiten, and Moose. — 2016
7. **BRICKERBOT** — A bot infecting IoT devices and rendering them inoperable. — 2017

MAJOR IOT SECURITY NEWS TIMELINE

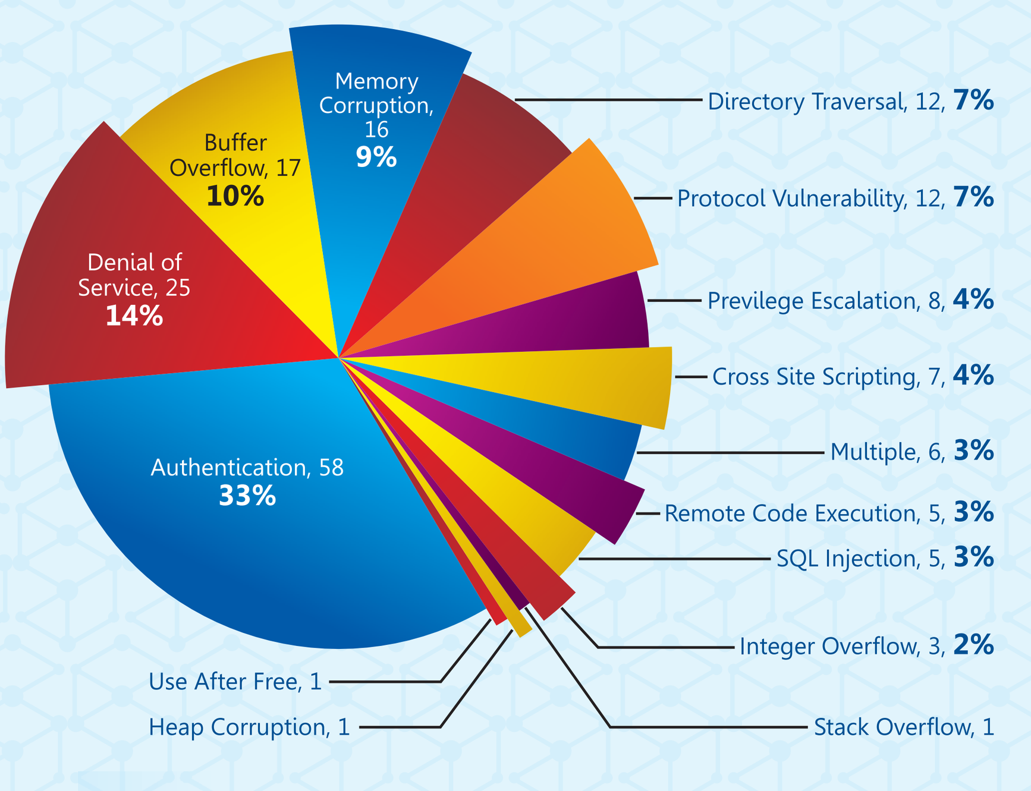
DATE	NAME	AFFECTED DEVICES	NUMBER OF DEVICES AFFECTED OR VULNERABLE	INFECTION METHOD
January 2010	Stuxnet	PLC/SCADA	Affected, 200,000+	Worm, spreads through removable drives
August 2013	Charlie Miller and Chris Valasek Auto Hack	Automobiles with cellular service or Wi-Fi network like General Motors' OnStar, Toyota's Safety Connect and Ford's SYNC	Recall of 1.4 million Cars by Fiat Chrysler	Remote exploitation to inject messages into the CAN bus of a car. Gives the attacker wireless control, via the Internet, to any of thousands of vehicles.
April 2014	Heartbleed	Embedded devices and computers that are unpatched or cannot be patched	Virtually all of the internet's biggest websites Vulnerable, Countless devices	Exploits weaknesses in the OpenSSL software library to extract passwords and other sensitive information from a targeted device.
September 2016	Medsec pacemaker vulnerablilities	Abbott/St. Jude Pacemakers	Vulnerable, 465,000	Using RF for improper authentication that can be compromised or bypassed, another flaw that could allow a nearby attacker to issue commands to drain the battery, as well as a flaw that allows sensitive patient information being transmitted without encryption.
October 2016	Mirai	IoT devices, mostly CCTV cameras and DVR's	Vulnerable, 5,000,000+	Malware, uses default credentials on IOT devices, or a TR- protocol exploit, then looks for other IOT devices to infect. Botnet generally used for DDOS attacks
March 2017	Brickerbot	IoT devices	Affected, possibly 2,000,000+	Malware, uses default credentials on IOT devices to permanently brick devices
May 2017	Wannacry	Embedded devices and computers using unpatched /older Windows OS.	Affected, 230,000+	Ransomware, propagates using EternalBlue, an exploit of Windows' Server Message Block (SMB) protocol
May 2017	Persirai	IP Cameras	Vulnerable, 120,000+	Malware, via open port from UPnP protocol
July 2017	Devils Ivy	Devices running gSOAP library	Vulnerable, possibly in the tens of millions	RCE on cameras allows an attacker to remotely access a video feed or deny the owner access to the feed.
September 2017	Blueborne	Bluetooth enabled devices	Vulnerable, 5.3 billion+	Vulnerabilities in Bluetooth protocol
October 2017	KRACK	Nearly every device that uses WiFi	Vulnerable, Nearly every device that uses WiFi	Vulnerability in WPA2 security protocol

TOP IOT VULNERABILITIES

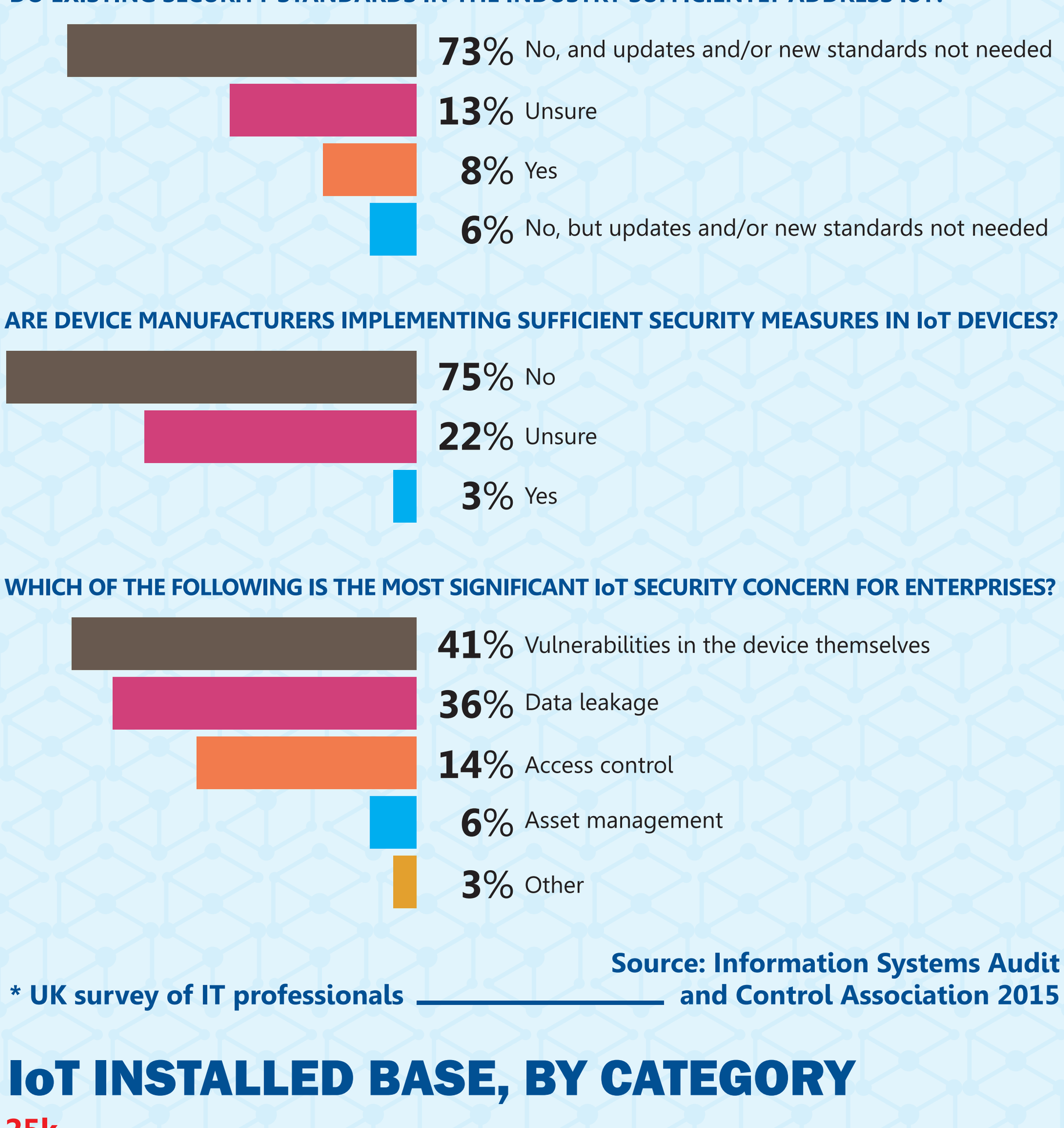
The OWASP Top 10 IoT Vulnerabilities from 2014 are as follows:

RANK	TITLE
1	Insecure Web Interface
2	Insufficient Authentication/Authorization
3	Insecure Network Services
4	Lack of Transport Encryption/Integrity Verification
5	Privacy Concerns
6	Insecure Cloud Interface
7	Insecure Mobile Interface
8	Insufficient Security Configurability
9	Insecure Software/Firmware
10	Poor Physical Security

VULNERABILITIES FOUND IN IOT/ICS/IIOT



IoT SECURITY*



* UK survey of IT professionals

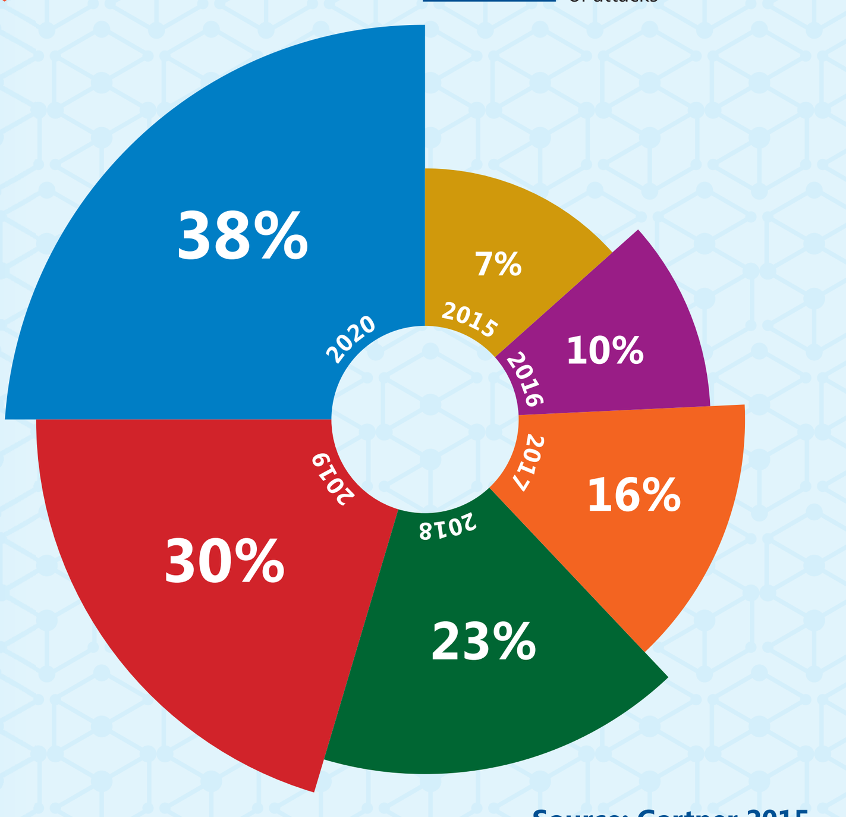
Source: Information Systems Audit and Control Association 2015

IoT SHARE OF THE GLOBAL CYBER-SECURITY MARKET

25% of identified enterprise attacks will involve the internet of things by 2020

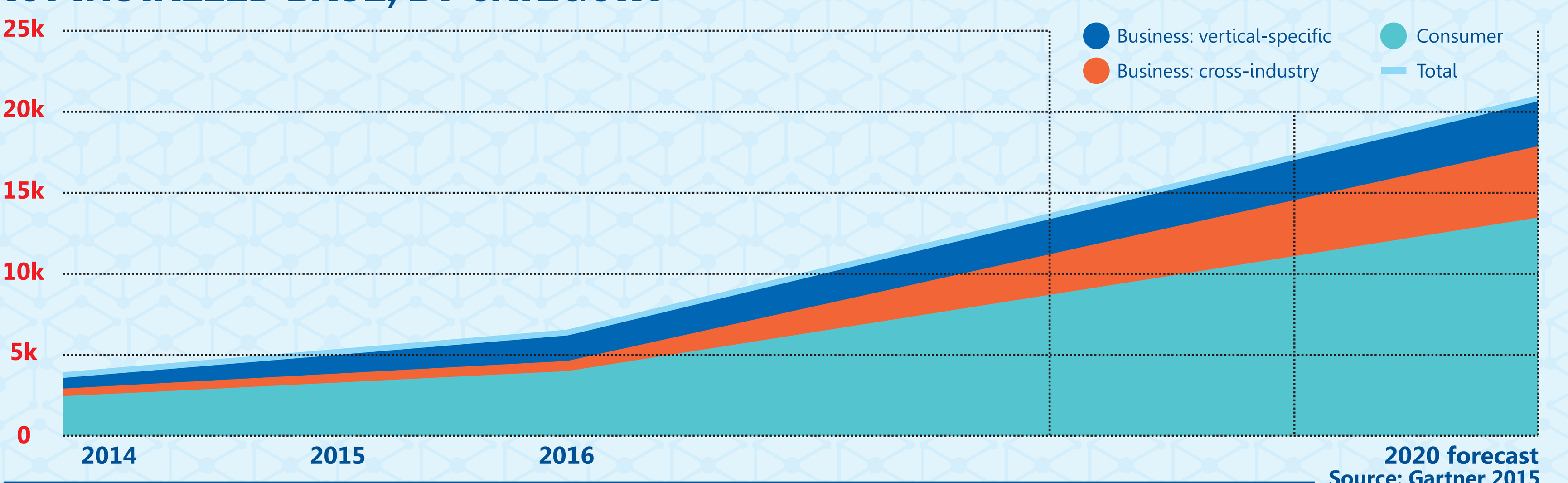
However...

only **10%** of IT security budgets will be spent on protecting against these types of attacks



Source: Gartner 2015

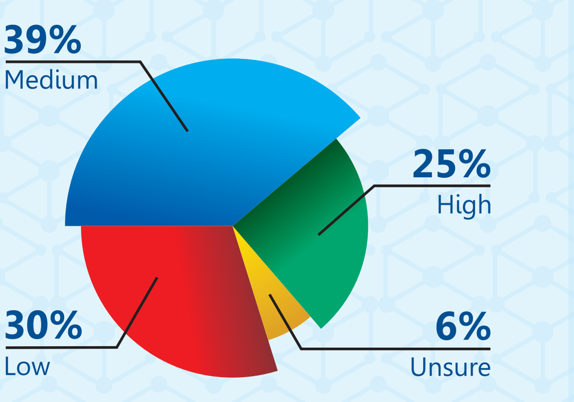
IoT INSTALLED BASE, BY CATEGORY



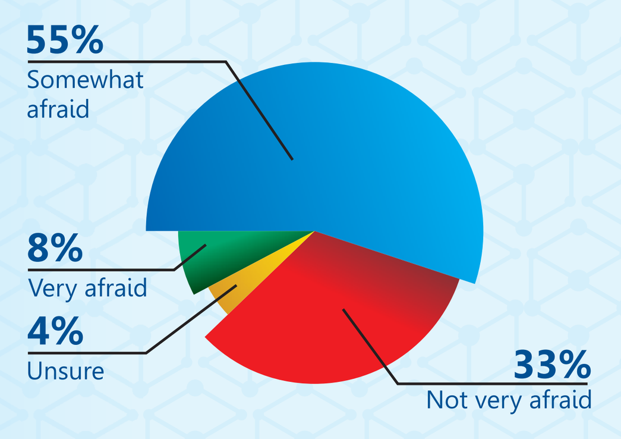
2020 forecast
Source: Gartner 2015

HACKING IoT DEVICES

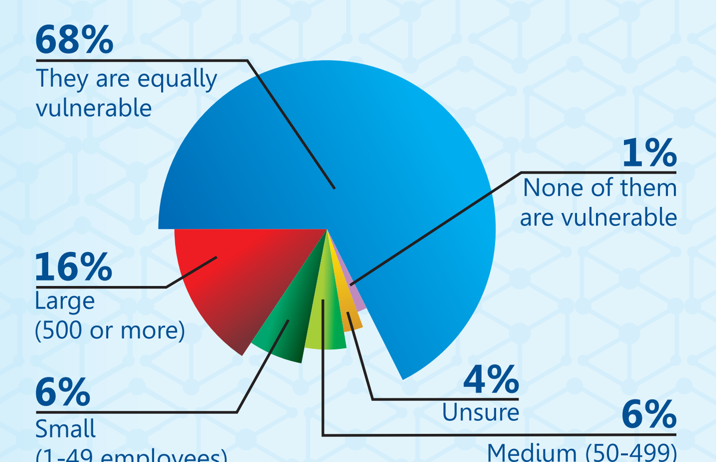
HOW LIKELY IS IT FOR A COMPANY TO BE HACKED THROUGH AN IoT DEVICE?



HOW AFRAID ARE YOU THAT YOUR IoT DEVICE MAY BE HACKED?



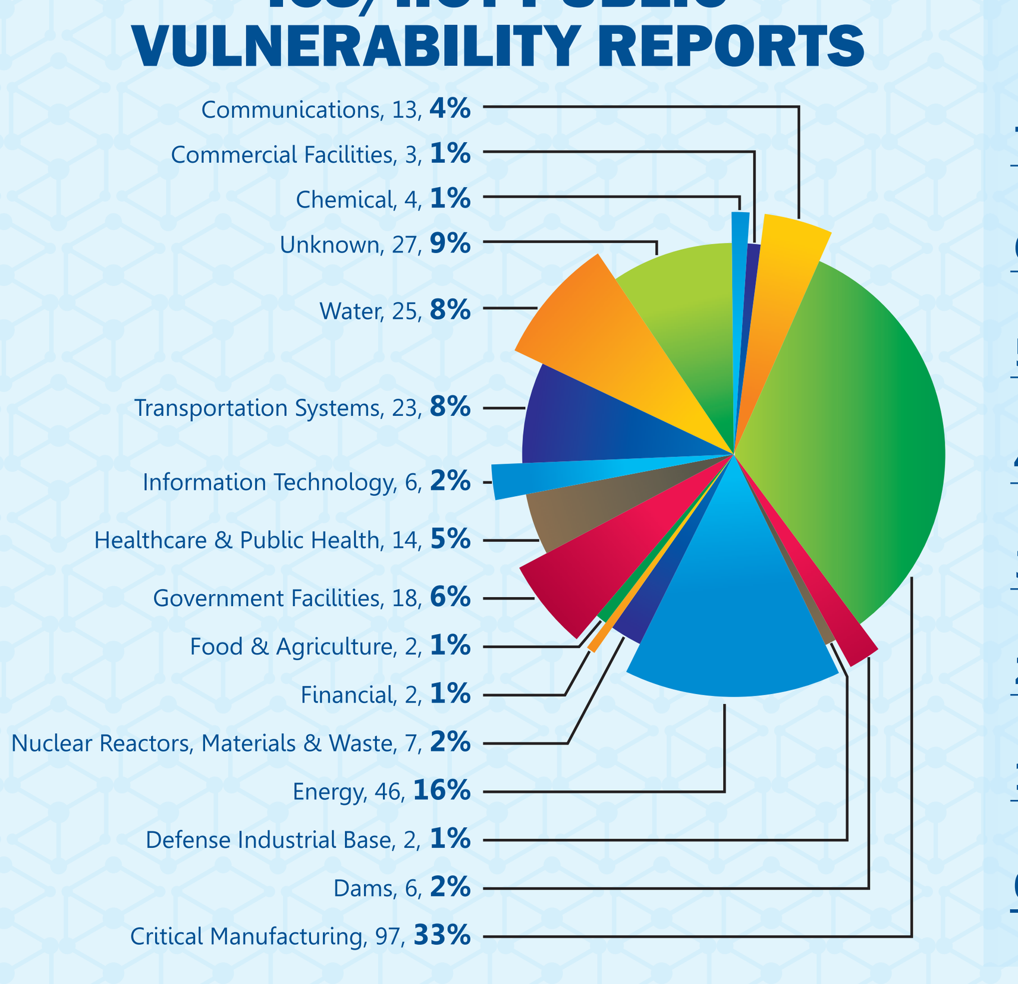
WHAT SIZE ENTERPRISE DO YOU THINK IS MOST VULNERABLE TO IoT-RELATED RISK?



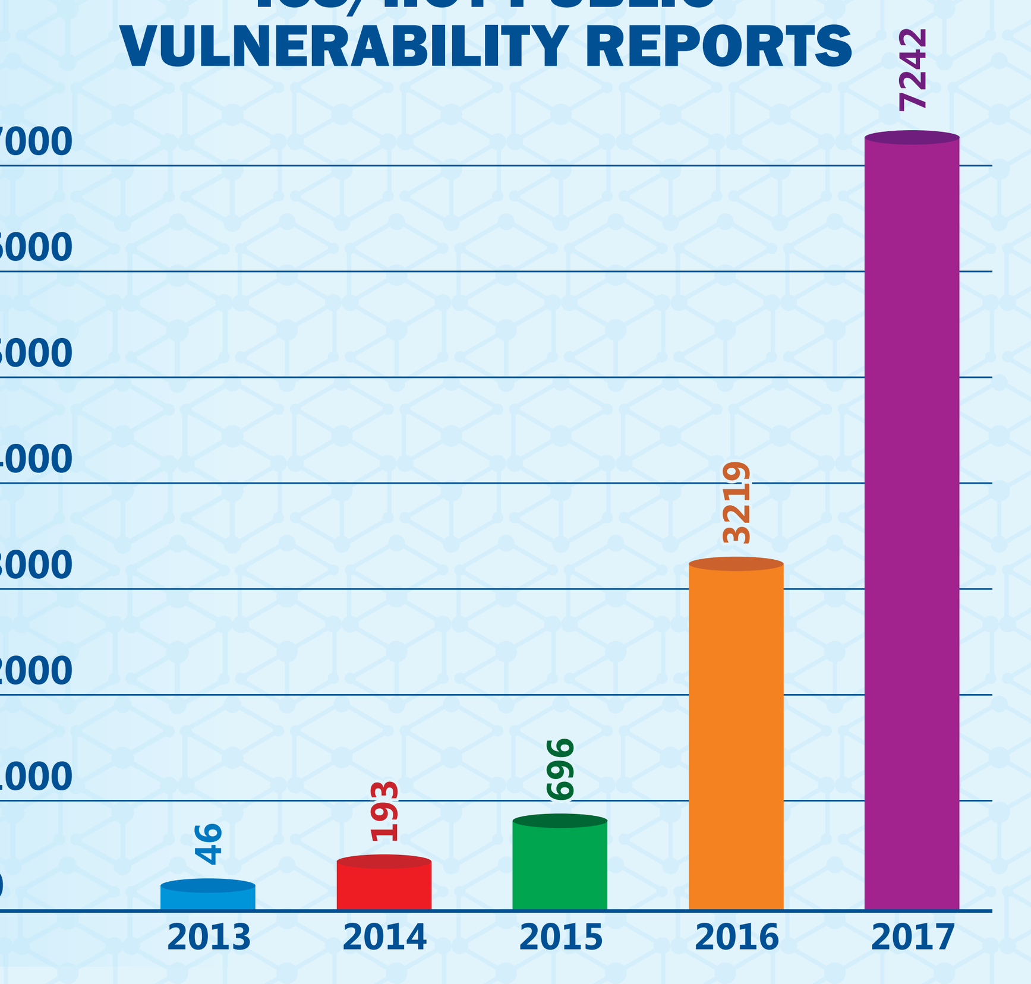
*UK survey of IT professionals

Source: Information Systems Audit and Control Association 2015

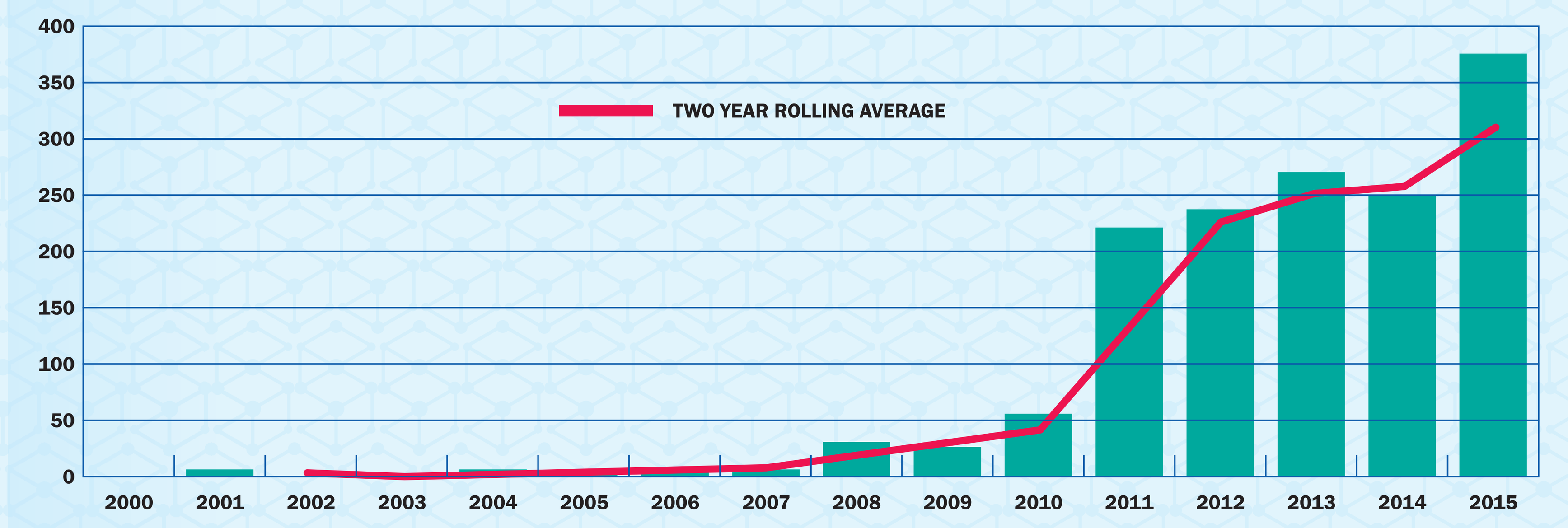
ICS/IIOT PUBLIC VULNERABILITY REPORTS



ICS/IIOT PUBLIC VULNERABILITY REPORTS



IIOT & INDUSTRIAL CONTROL REPORTED COMPROMISES/INCIDENCES



SENRIO
http://iot.security