The year the Internet fell apart
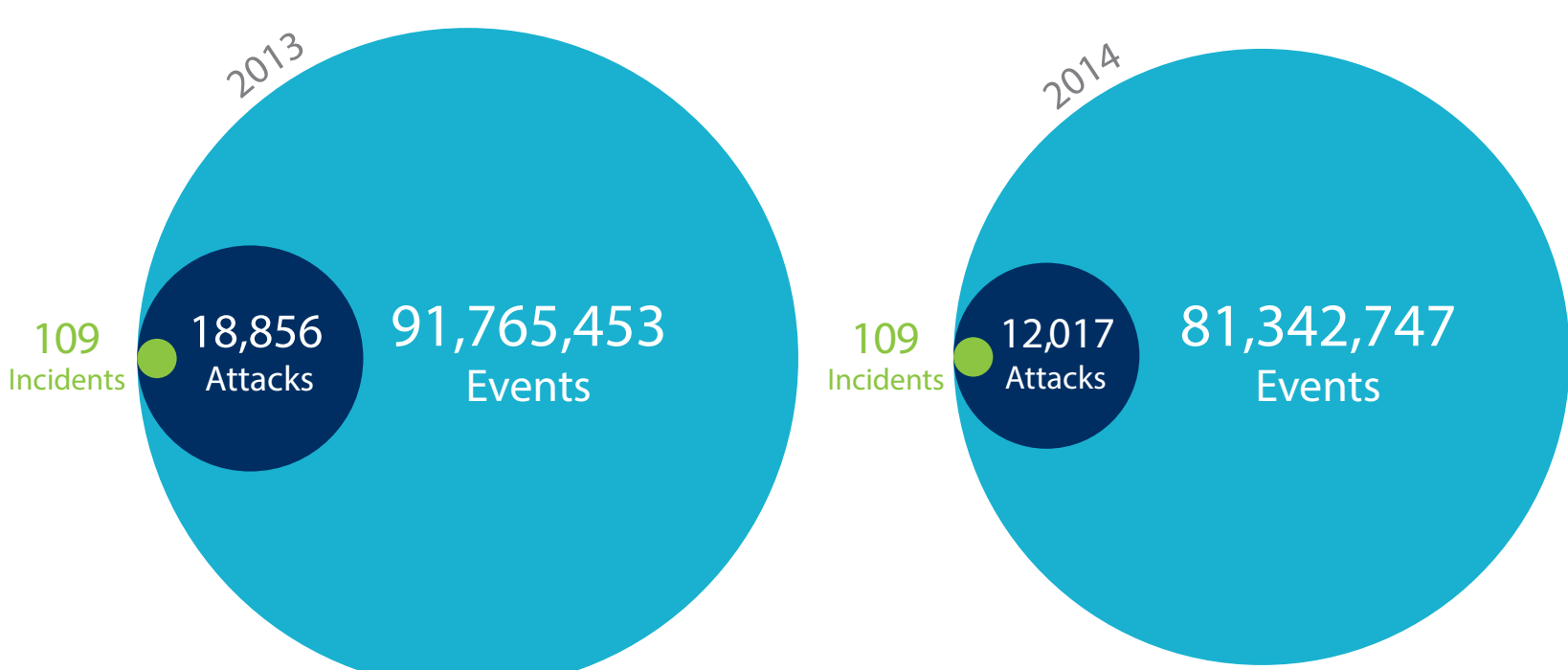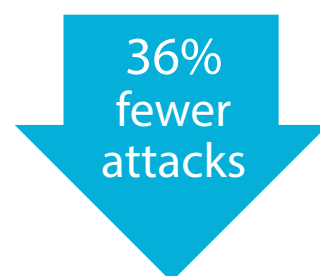
Significant threats and massive data breaches made front-page news on a regular basis in 2014
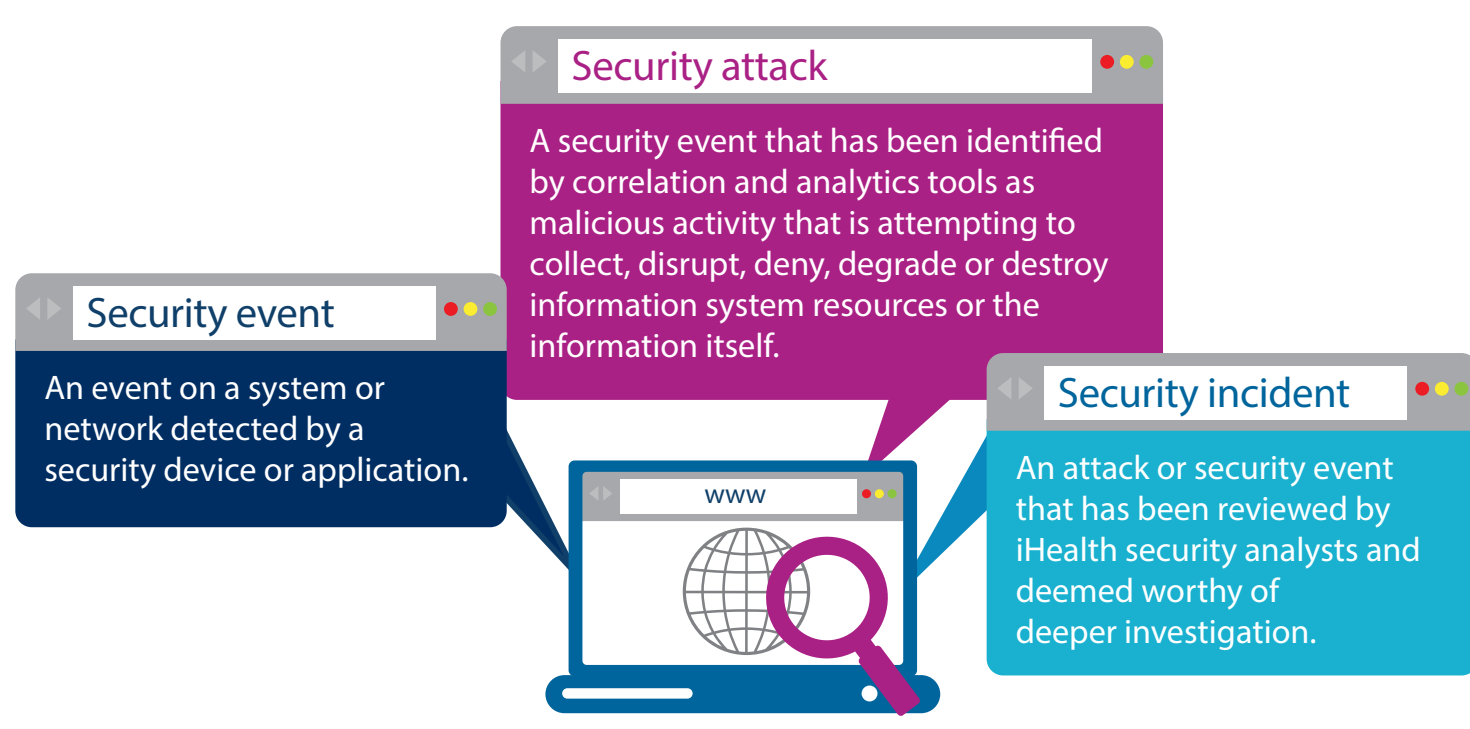
HOSPITAL CHAIN FEELS PAIN OF BREACH

CYBER ATTACK HITS HOME

THE ART OF THE HACK

Annual security events, attacks and incidents

2013
109 Incidents
18,856 Attacks
91,765,453 Events

2014
109 Incidents
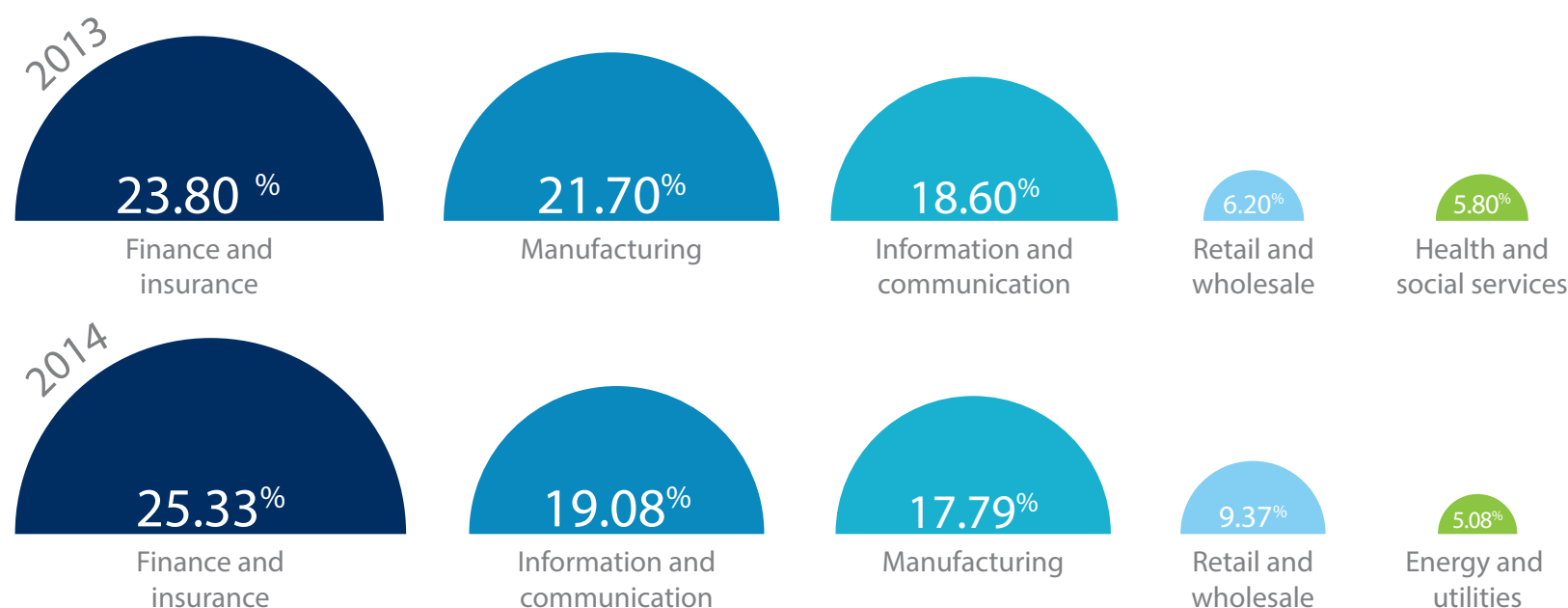12,017 Attacks
81,342,747 Events

iHealth security intelligence saw the average number of security events in any one of our clients' systems drop to 81 million in 2014—from nearly 92 million in 2013, yielding 36% fewer attacks, but the same number of incidents.

36% fewer attacks

Events, attacks and incidents defined

Security attack
A security event that has been identified by correlation and analytics tools as malicious activity that is attempting to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Security event
An event on a system or network detected by a security device or application.

www

Security incident
An attack or security event that has been reviewed by iHealth security analysts and deemed worthy of deeper investigation.

Over 62% of incidents targeted just 3 industries in 2014

2013
23.80% Finance and insurance
21.70% Manufacturing
18.60% Information and communication
6.20% Retail and wholesale
5.80% Health and social services

2014
25.33% Finance and insurance
19.08% Information and communication
17.79% Manufacturing
9.37% Retail and wholesale
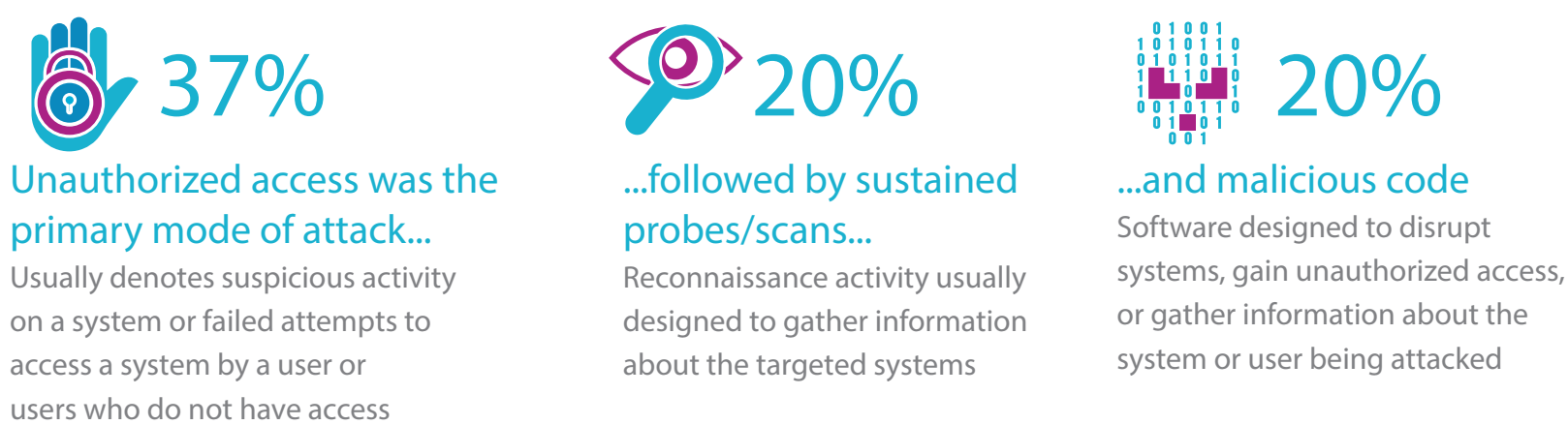5.08% Energy and utilities

Retail took a hammering—thanks to point-of-sale malware

Unauthorized access and malicious code accounted for nearly half of the incidents in energy and utilities

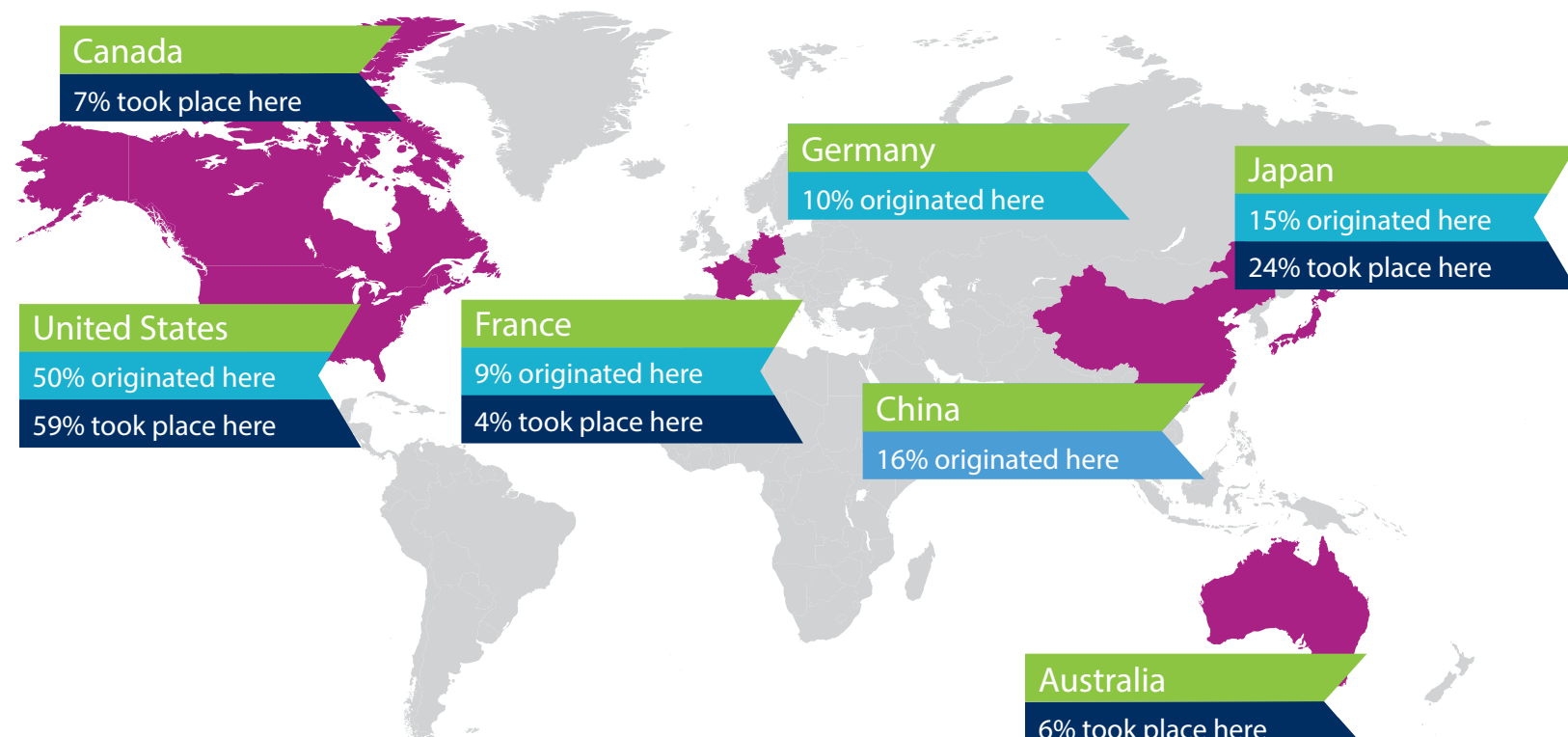## Unauthorized access was nearly twice as prevalent in 2014 as in 2013 among the top 5 industries

37%
Unauthorized access was the primary mode of attack...
Usually denotes suspicious activity on a system or failed attempts to access a system by a user or users who do not have access

20%
...followed by sustained probes/scans...
Reconnaissance activity usually designed to gather information about the targeted systems

20%
...and malicious code
Software designed to disrupt systems, gain unauthorized access, or gather information about the system or user being attacked

Who are the "bad guys"? More than half are insiders*

* Anyone who has physical or remote access to a company's assets

45% Outsiders

31.5% Malicious insiders

23.5% Inadvertent actor
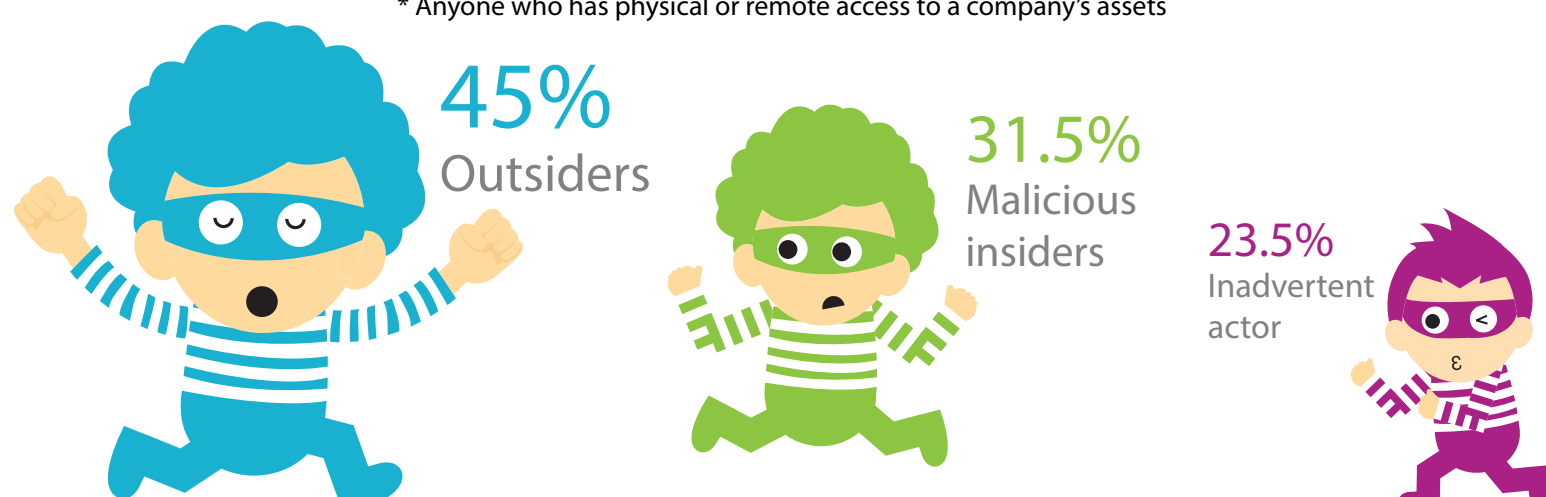
Whether they're malicious insiders or inadvertent actors, they pose a big security risk

Where are these attacks coming from? And where are they taking place?

Canada
7% took place here

Germany
10% originated here

Japan
15% originated here
24% took place here

United States
50% originated here
59% took place here

France
9% originated here
4% took place here

China
16% originated here

Australia
6% took place here

The largest number of attacks both originated and took place in the US

Learn more

iHealth Innovative Solutions

SEJ03278-USEN-01