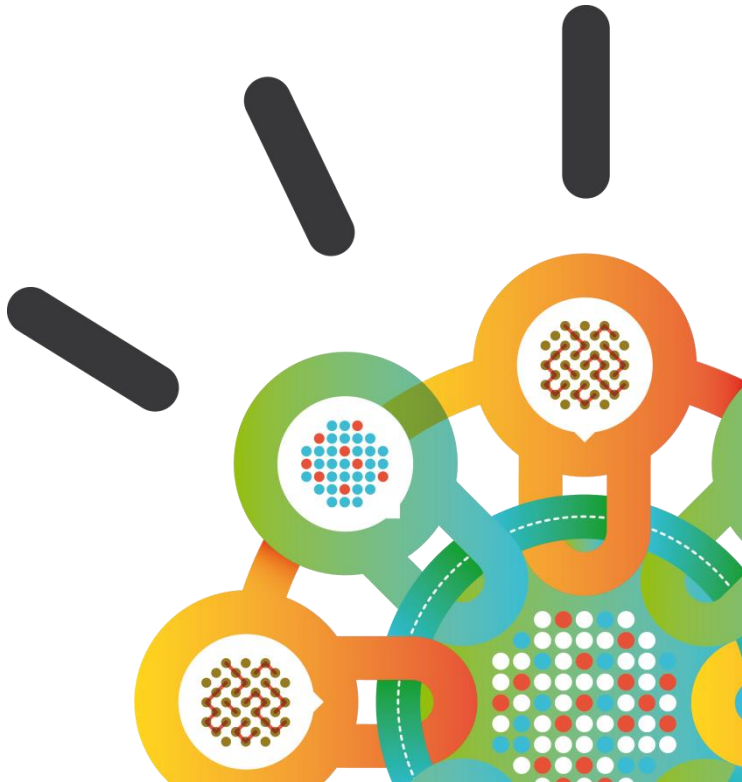
Security Intelligence.
Think Integrated.

The Emerging Threat Landscape

IBM X-Force

[name]
[title]

September 29, 2014



IBM X-Force

is the foundation for advanced security and threat research across the IBM Security Framework.

IBM X-Force® Research and Development

Expert analysis and data sharing on the global threat landscape

The IBM X-Force Mission

- **Monitor** and evaluate the rapidly changing threat landscape
- **Research** new attack techniques and develop protection for tomorrow's security challenges
- **Educate** our customers and the general public
- **Integrate** and distribute Threat Protection and Intelligence to make IBM solutions smarter

IBM X-Force monitors and analyzes the changing threat landscape.

Coverage

20,000+ devices under contract

15B+ events managed per day

133 monitored countries (MSS)

3,000+ security related patents

100M+ customers protected from fraudulent transactions

Depth

23B+ analyzed web pages and images

8M+ spam and phishing attacks daily

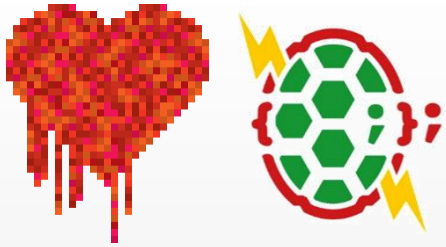
83K+ documented vulnerabilities

860K+ malicious IP addresses

Millions of unique malware samples

2014 has been defined by …

High Impact Vulnerability Disclosures



Heartbleed and Shellshock have had a massive impact in the infrastructure of the internet.

What are the long term repercussions?

Massively Distributed APTs

Banking Trojans are being repurposed with expanded capabilities into massively distributed APT malware to attack enterprises in other industries.

Is your organization at risk?

Ongoing, Costly Data Breaches

Community Health Service had a breach of 4.5M patient records. Home Depot had a breach of 56M credit card records. JP Morgan just announced the leak of 76M records.

How can you protect your sensitive data?

We are in an era of continuous breaches.

Attackers are relentless, victims are targeted, and the damage toll is rising

Operational Sophistication

IBM X-Force® declared **Year of the Security Breach**

Near Daily Leaks of Sensitive Data

40% increase in reported data breaches and incidents

Relentless Use of Multiple Methods

500,000,000+ records were leaked, while the future shows no sign of change

Source: IBM X-Force Threat Intelligence Quarterly – 1Q 2014

Note: Size of circle estimates relative impact of incident in terms of cost to business.

There was a decline in vulnerability disclosures in the first half of 2014; this could be the first reduction since 2011.

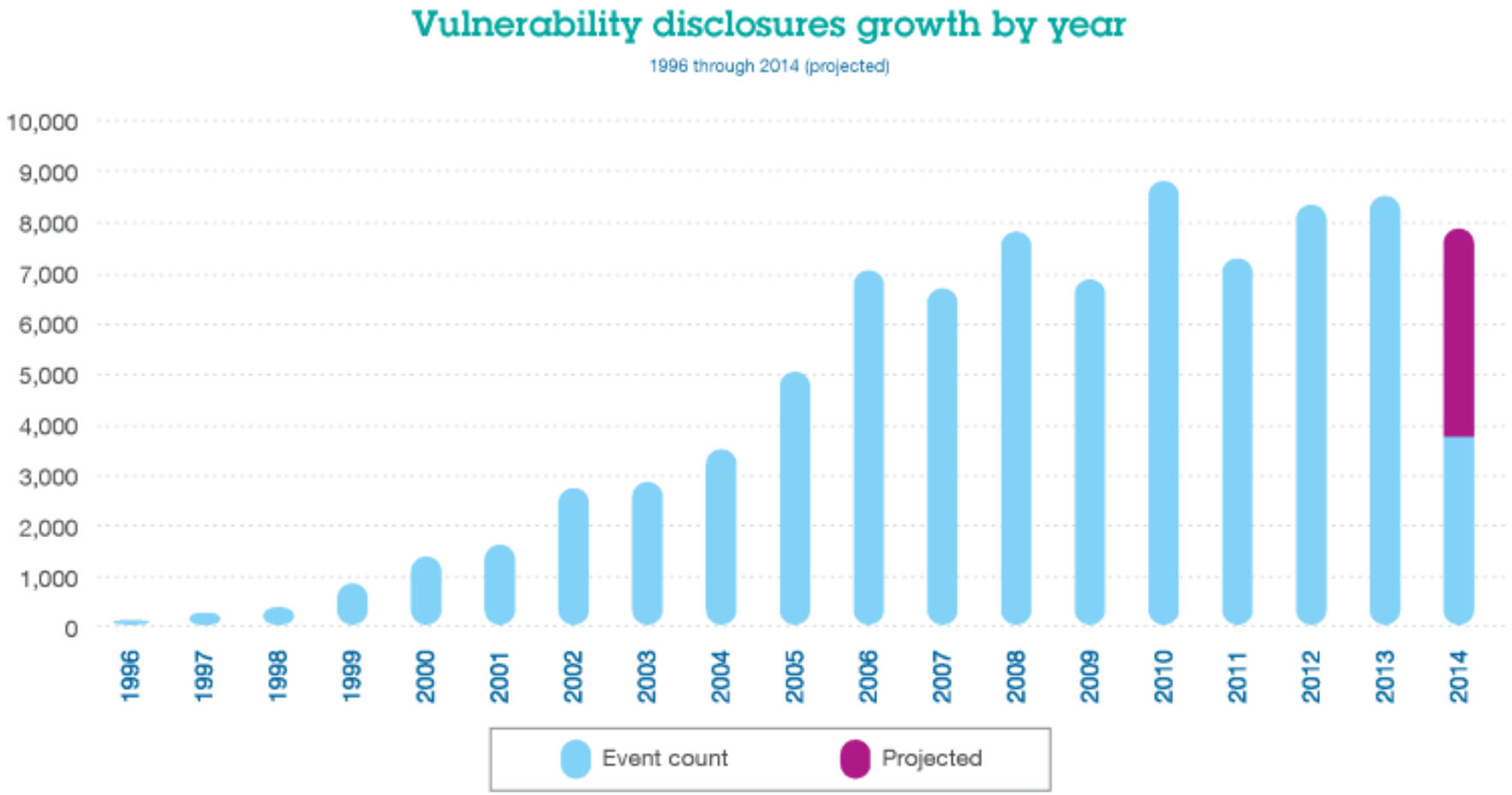


Figure 6. Vulnerability disclosures growth by year, 1996 through 2014 (projected)

It is difficult to point to any one factor that has contributed to the decline in the number of vulnerability disclosures in 1H 2014.

A decreasing number of vendors consistently reporting vulnerabilities might be contributing to the recent decline in total overall vulnerabilities disclosed.

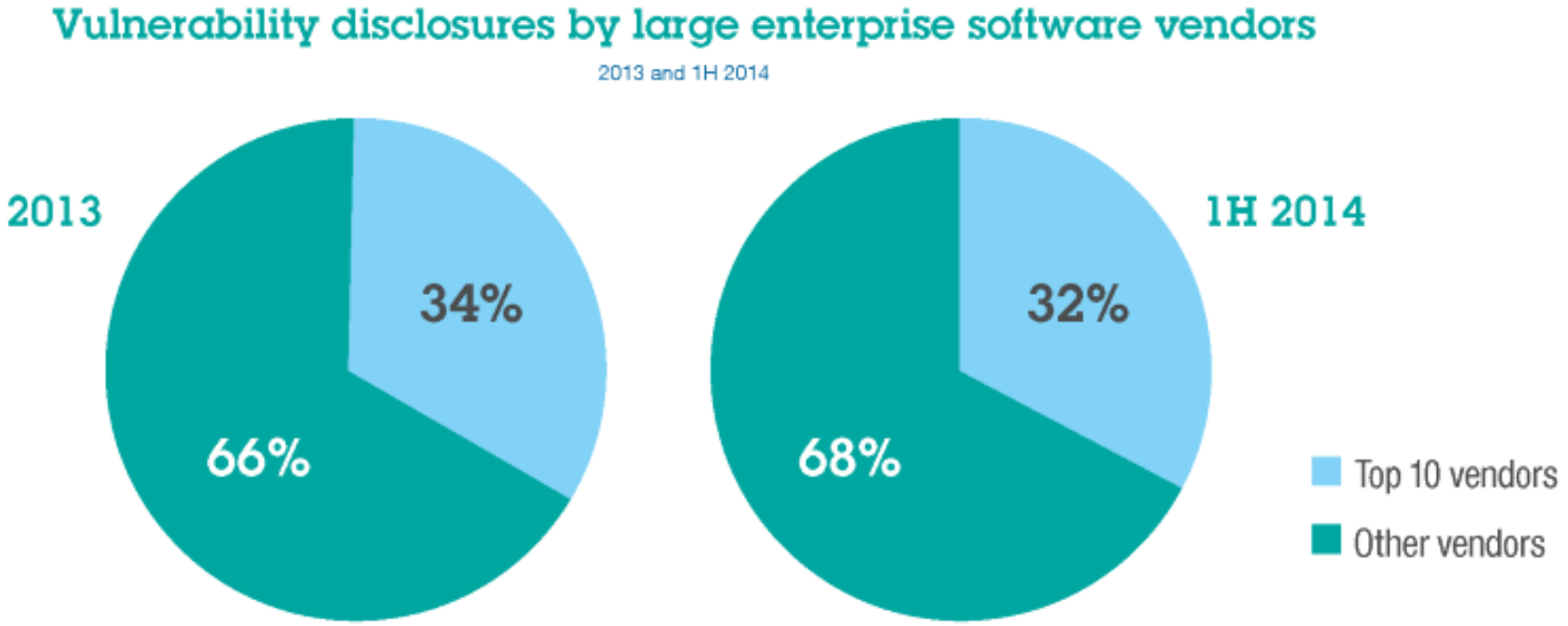
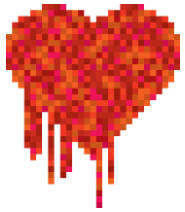


Figure 7. Vulnerability disclosures by large enterprise software vendors, 2013 and 1H 2014

Source: IBM X-Force® Research and Development

Does CVSS scoring represent risk to networks and systems?

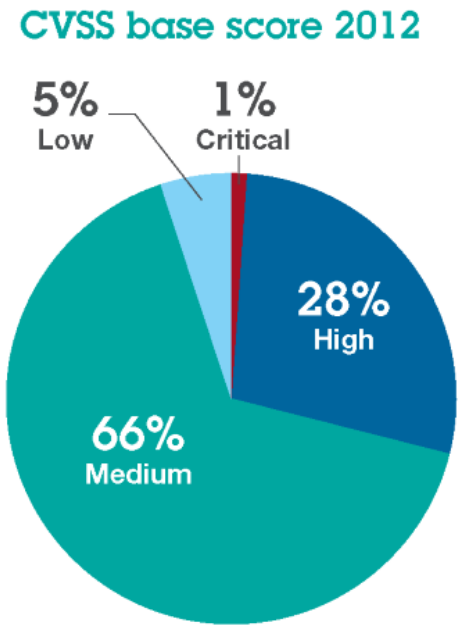
CVSS Base Score

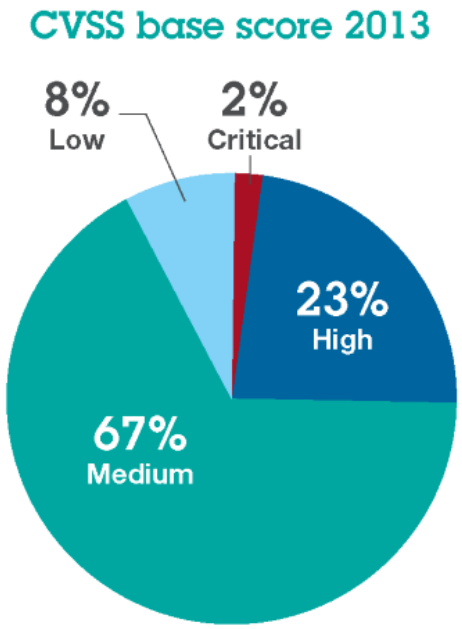


5.0

10.0

The time and attention IT teams spent patching systems and responding to customer inquiries, as well as the potential sensitivity of data exposed, the true impact of Heartbleed was greater than the CVSS base score would indicate.





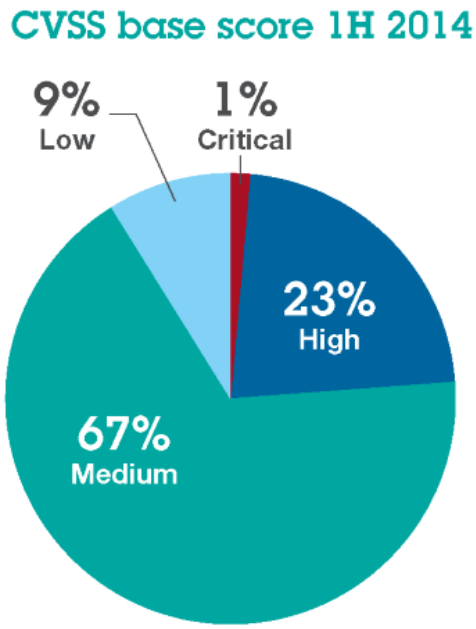
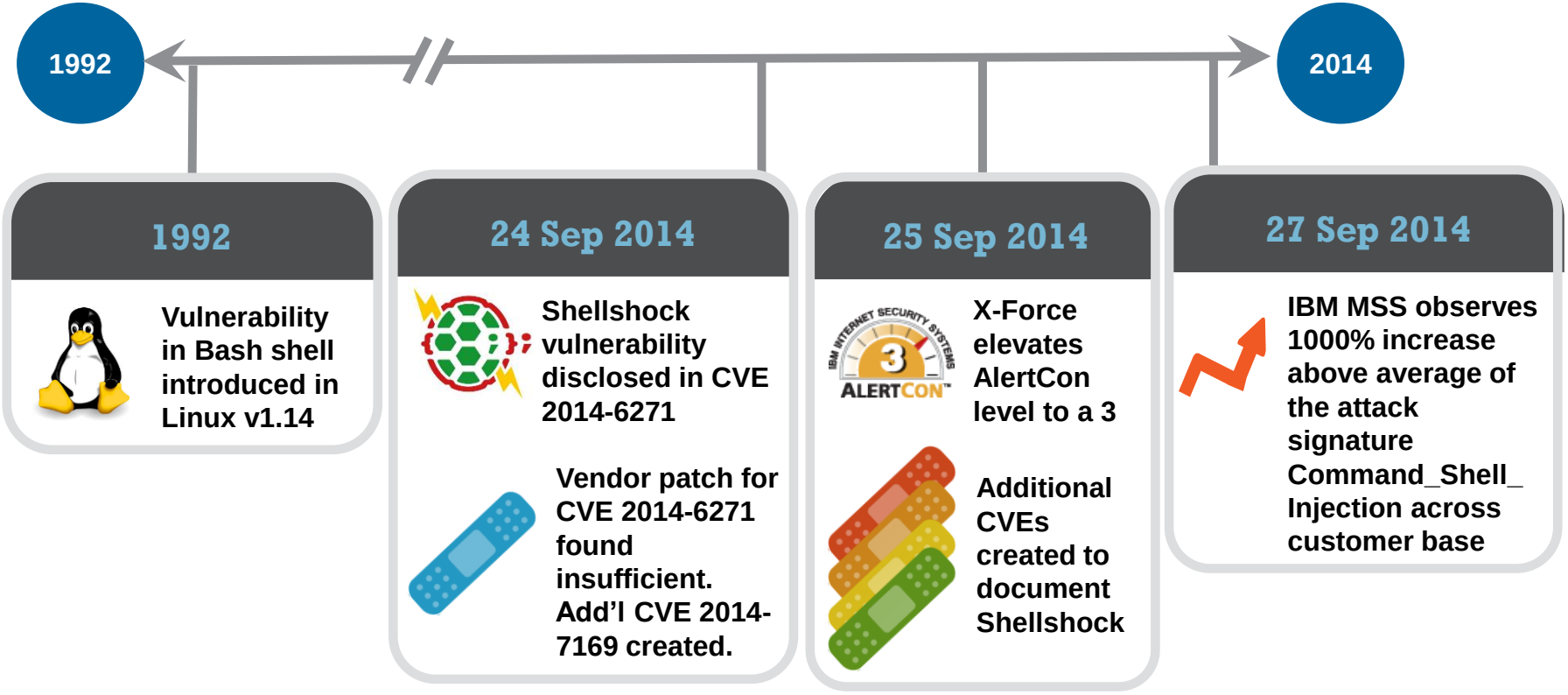


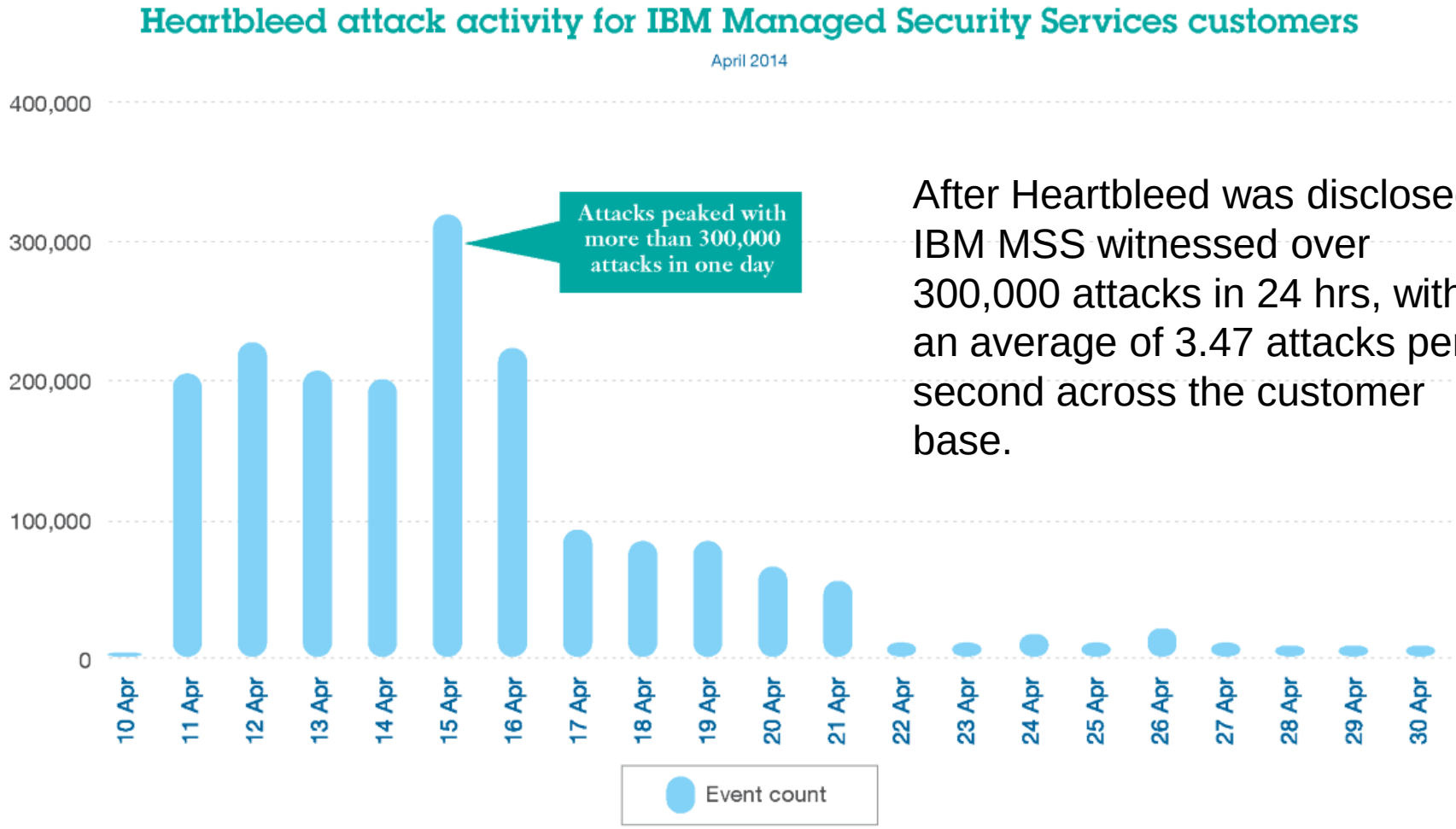
Figure 9. CVSS base scores, 2012 through 1H 2014

The disclosure of the Shellshock bug in September brought immediate exploit attempts.

Patching the original vulnerability was complicated by the development of additional exploit techniques, resulting in additional CVE numbers created



Heartbleed attacks surged to 3.47 attacks per second after the vulnerability disclosure.



After Heartbleed was disclosed, IBM MSS witnessed over 300,000 attacks in 24 hrs, with an average of 3.47 attacks per second across the customer base.

Figure 1. Attack activity related to the Heartbleed vulnerability, as noted for IBM Managed Security Services customers, in April 2014

Source: IBM X-Force® Research and Development

IBM MSS continues to average 7k attacks per day – mostly from malicious hosts.

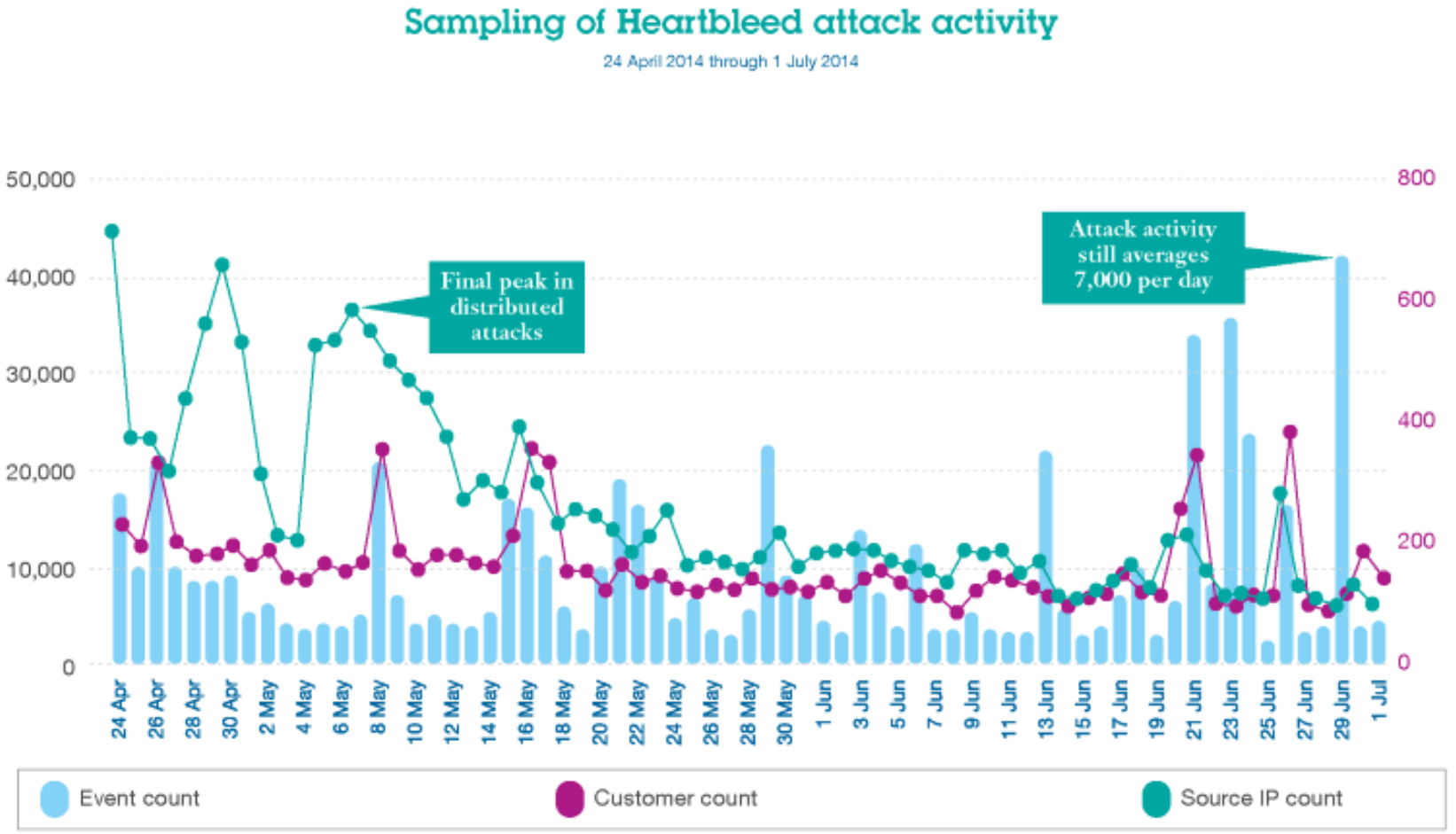
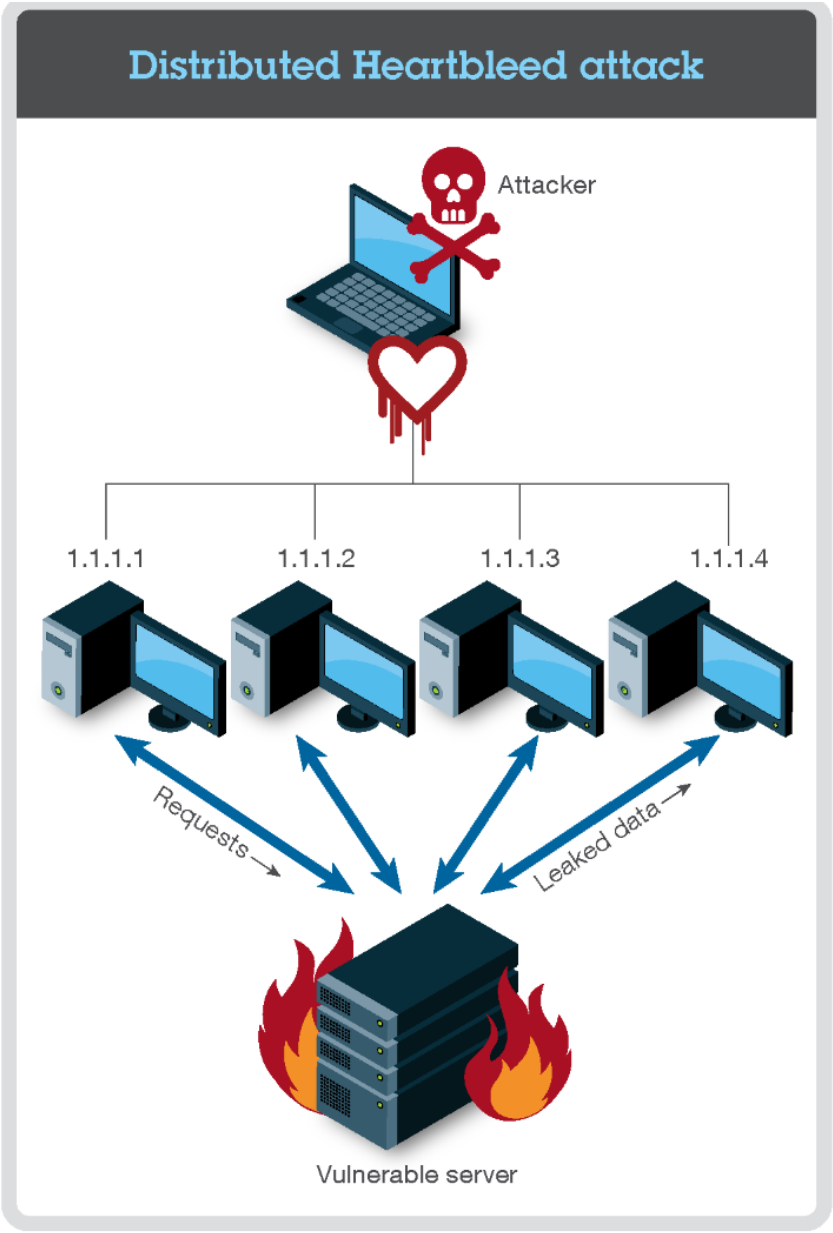


Figure 3. Sampling of Heartbleed attack activity for IBM Managed Security Services customers, 24 April 2014 through 1 July 2014

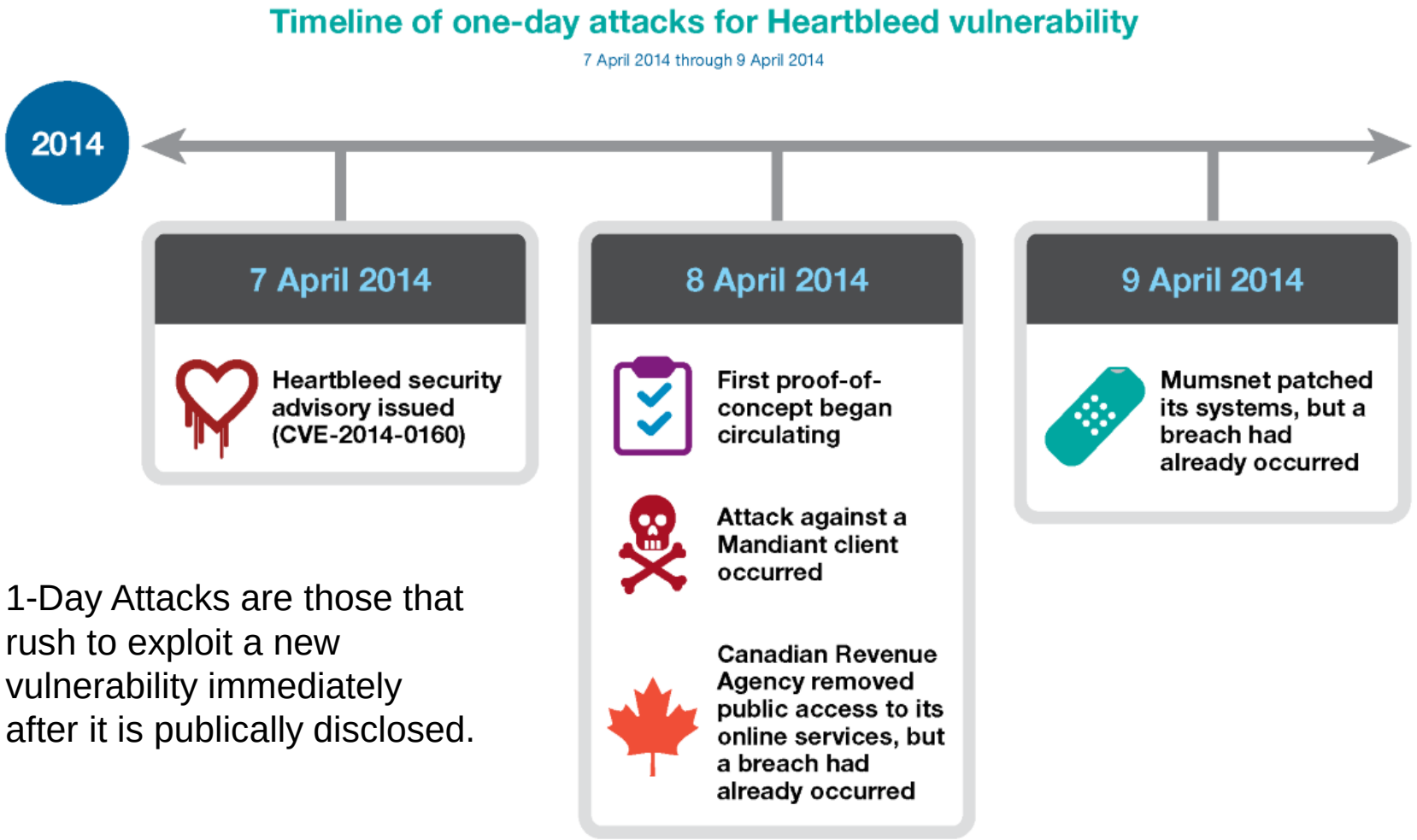
Source: IBM X-Force® Research and Development

Rather than a single IP address executing the attack repeatedly, many of the attacks used a distributed method.

This enabled attackers to have a large, diversified attack surface and the flexibility to overcome rudimentary blocking strategies.



One-day attack methods demonstrate how quickly attackers rush to exploit a vulnerability like Heartbleed.

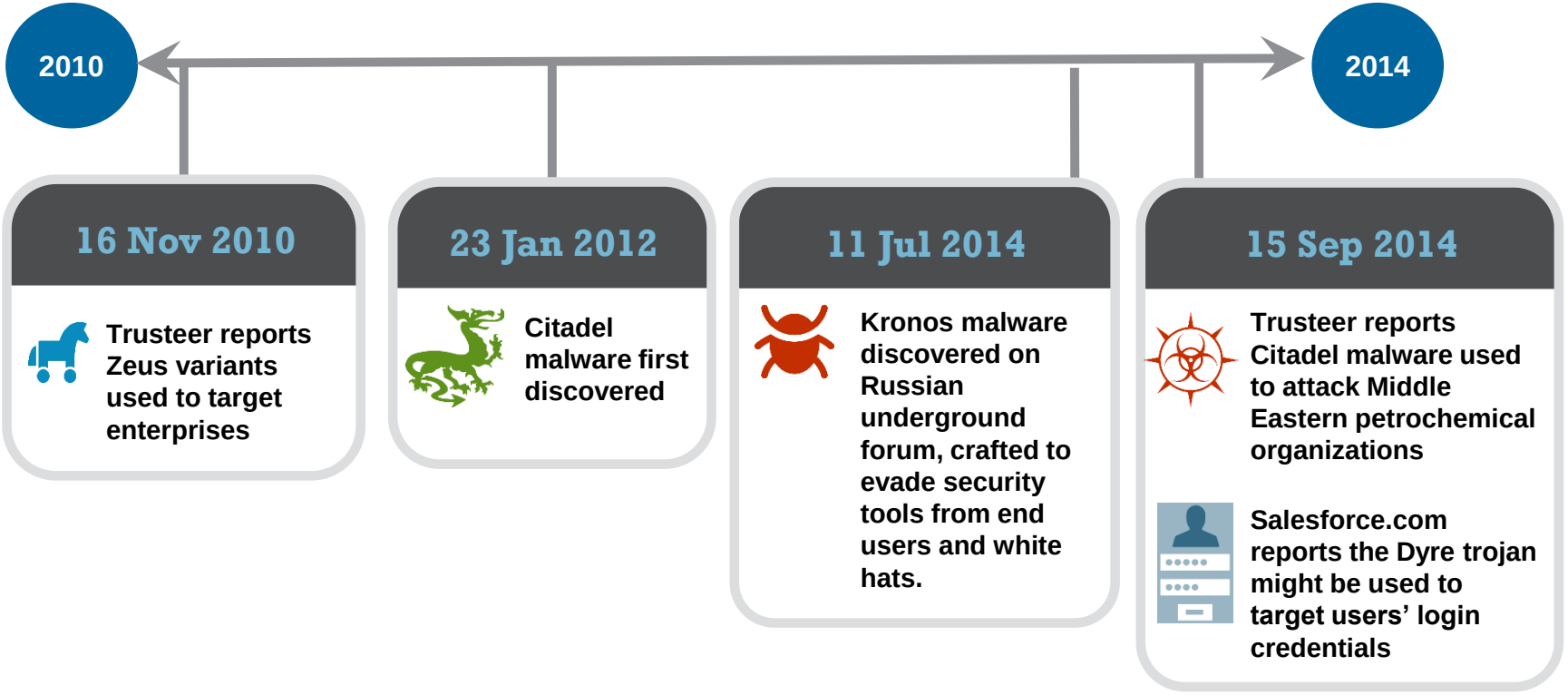


1-Day Attacks are those that rush to exploit a new vulnerability immediately after it is publically disclosed.

Figure 4. Timeline of one-day attacks for Heartbleed vulnerability (CVE-2014-0160), 7 April 2014 through 9 April 2014

To take advantage of vulnerabilities in enterprise networks, banking Trojans are being repurposed into massively distributed APT malware.

Trojans like Citadel, Dyre, Zeus, SpyEye, and Shylock are being used to infiltrate enterprises beyond the banking industry.



These variants use mass distribution techniques to infiltrate organizations with expanded functionality.

Mass distribution techniques:

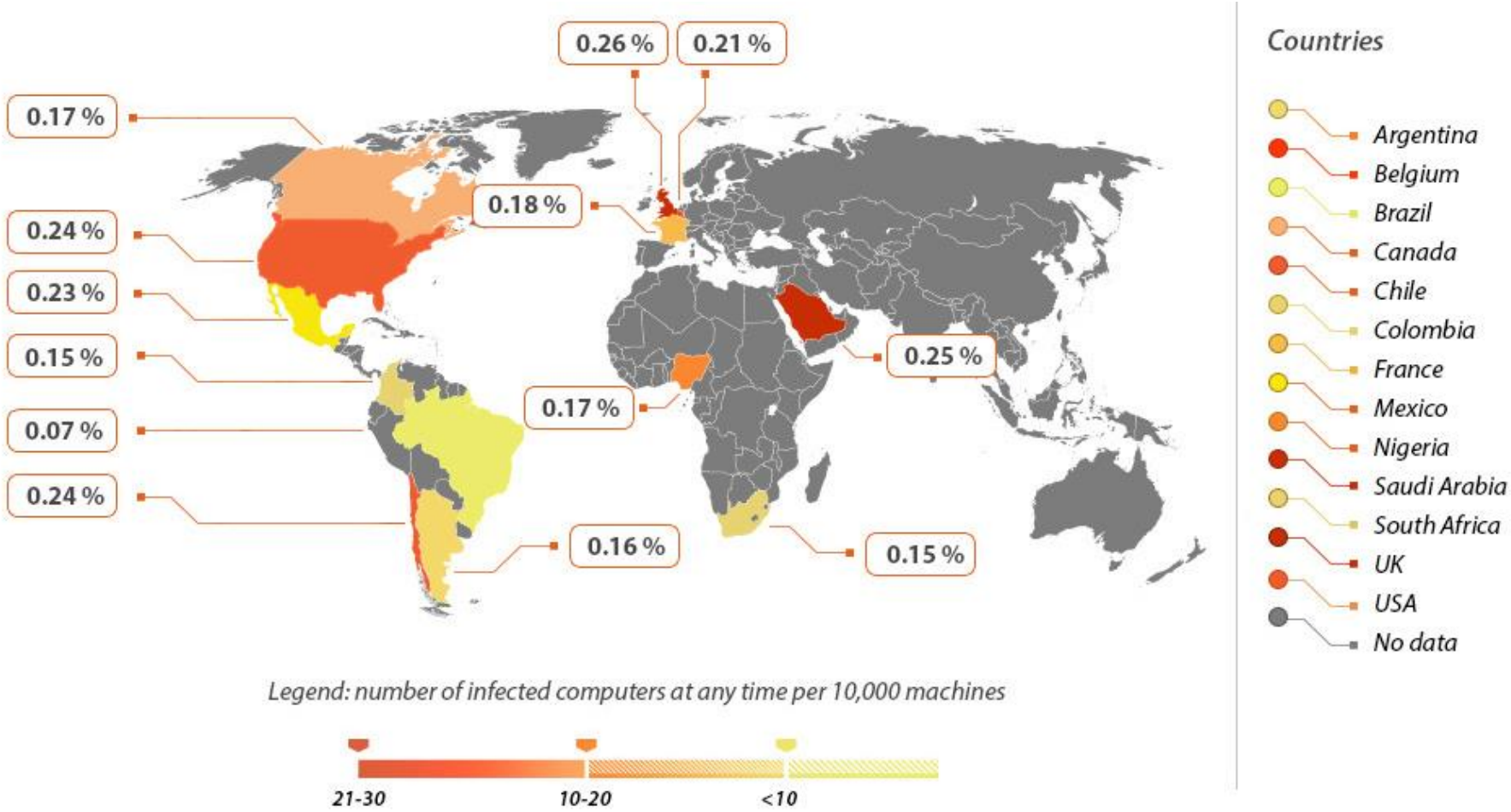
- Malicious email attachments
- Drive-by downloads
- Watering hole attacks
- Social-engineering schemes

Expanded functionality:

- Keylogging
- Screenshot capturing
- Video capturing
- Form grabbing
- HTML injection
- Remote execution of command line instructions
- Remote control of the infected machine
- Advanced evasion techniques
- Anti-research techniques

An average of 1 in 500 machines is infected with massively distributed APT malware at any point in time.

Infection Rates for Massively Distributed APT Malware by Country



Sophisticated attack methods are creating massive breaches across industries.

Healthcare April 2014	*An APT group used sophisticated malware to steal 4.5M patient records*	**Fashion & discount stores** April 2014	*Data on three million customer payment cards stolen in a breach over several months*
Grocery & drug chain August 2014	*Unlawful intrusion to obtain credit and debit card payment data*	**Consumer products & hospitality** August 2014	*33 restaurants across the country were affected by the breach of credit card information*
Grocery & drug chain August 2014	*Cash register system breached by hackers resulting in the theft of credit and debit card information*	**Home improvement stores** September 2014	*Payment systems were breached stealing 56M cards at nearly 2,200 U.S. and Canadian stores during a four month attack*

Global and country-level averages show that the cost of a data breach is on the rise.

Cost per record* in 2013

Global average

$145

9%

year-to-year increase

Highest countries

$201 in the U.S.

$195 in Germany

$70 in Brazil

$51 in India

Lowest countries

Cost per incident* in 2013

Global average

$3.5M

15%

year-to-year increase

Highest countries

$5.9M in the U.S.

$4.7M in Germany

$1.6M in Brazil

$1.4M in India

Lowest countries

*Currencies converted to US dollars

Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, sponsored by IBM

Highly regulated industries have the highest per-record data breach costs.

$359
Healthcare

$294
Education

$227
Pharmaceutical

$206
Financial

$155
Consumer

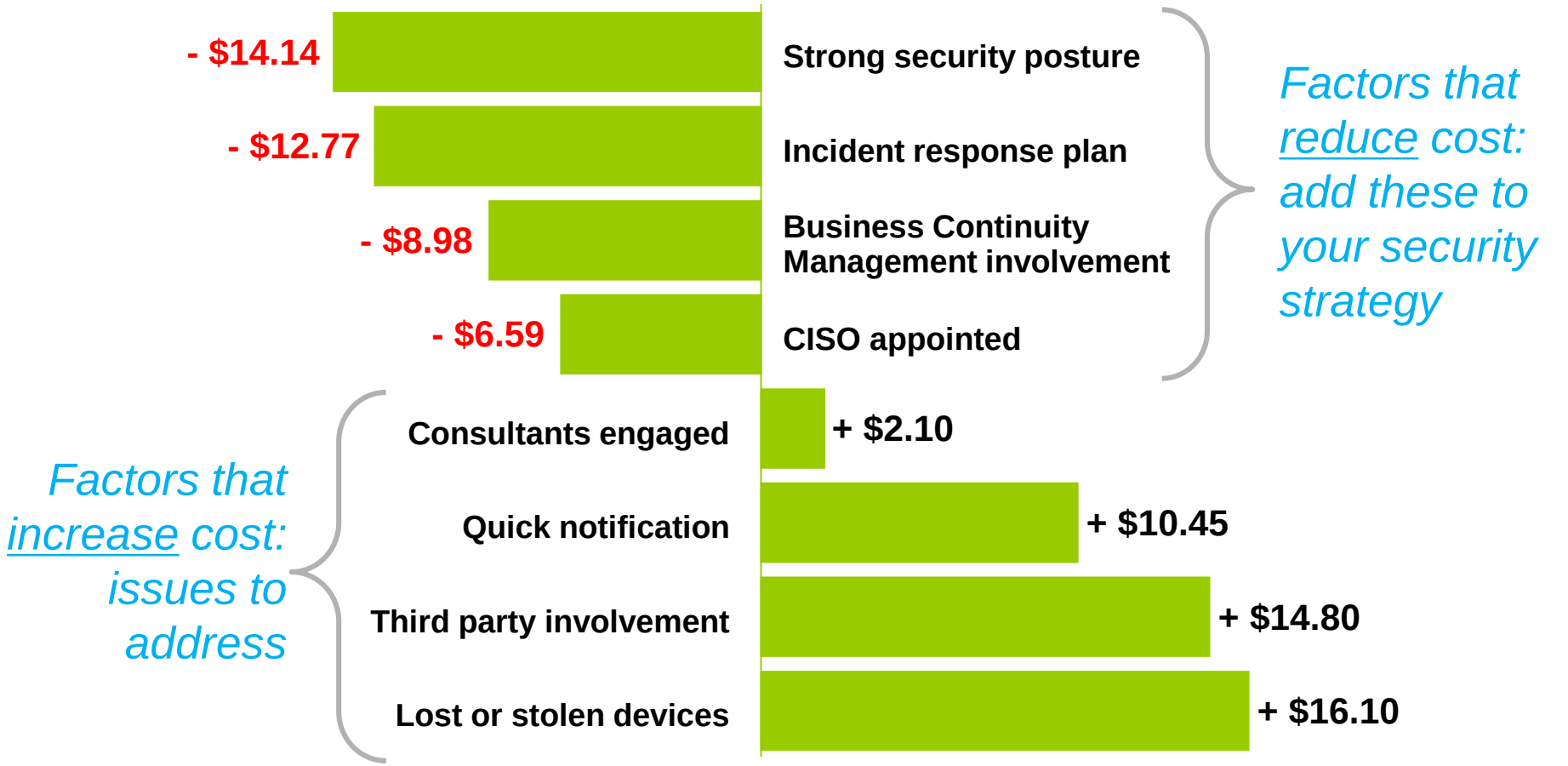
$141
Energy

$122
Hospitality

$105
Retail

*Currencies converted to US dollars
Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, sponsored by IBM

You can raise or lower your per-record cost of a data breach by addressing these eight influencing factors.

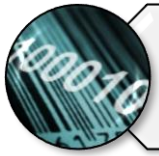


*Currencies converted to US dollars

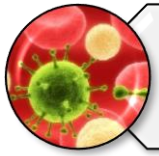
Source: 2014 Cost of Data Breach Study: Global Analysis, Ponemon Institute, sponsored by IBM

What can you do to mitigate these threats?

Keep up with threat intelligence.



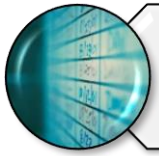
Maintain a current and accurate asset inventory.



Have a patching solution that covers your entire infrastructure.

Implement mitigating controls.

Instrument your environment with effective detection.



Create and practice a broad incident response plan.

Connect with IBM X-Force Research & Development

Twitter
@ibmsecurity and @ibmxforce

IBM X-Force Threat Intelligence
Reports and Research
http://www.ibm.com/security/xforce/

IBM X-Force Security Insights Blog
www.SecurityIntelligence.com/topics/x-force

Find more on SecurityIntelligence.com

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed or misappropriated or can result in damage to or misuse of your systems, including to attack others. No IT system or product should be considered completely secure and no single product or security measure can be completely effective in preventing improper access. IBM systems and products are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT SYSTEMS AND PRODUCTS ARE IMMUNE FROM THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Thank You

www.ibm.com/security