Managing Risk in Digital Transformation:
Peeking to the future of Cyber Insurance

July 24, 2019

Huge Spend on Digital Transformation; Cybersecurity Spend Not Aligned

Spending on Innovation

Spending/Focus on Cybersecurity Not Aligned

40%
of all technology spending will go toward digital transformations.

-IDC

$2T
the amount enterprises will spend on digital transformations by 2019.

-IDC

79%
of organizations are adopting new and emerging technologies faster than they can address related security issues.

-Accenture

<10%
of organizations spent more than 10% of their budget aligning cyber initiatives to their digital transformation efforts.

-Deloitte

1780s	1870s	1970s	Today
Industry 1.0	**Industry 2.0**	**Industry 3.0**	**Industry 4.0**
Mechanization Water Power Steam Power	**Mass Production Assembly Line Electrical Energy**	**Automation Computers Electronics**	**Internet of Things Big Data**

Incidents in the Headlines

BUSINESS

Marriott Says Starwood Data Breach Affects Up to 500 Million People

Hacked information includes passport numbers, payment-card numbers in addition to addresses, travel details

BUSINESS

British Airways Says Data Breach Larger Than Estimated

Announcement came after Cathay Pacific said 9.4 million passenger records were compromised in a separate attack
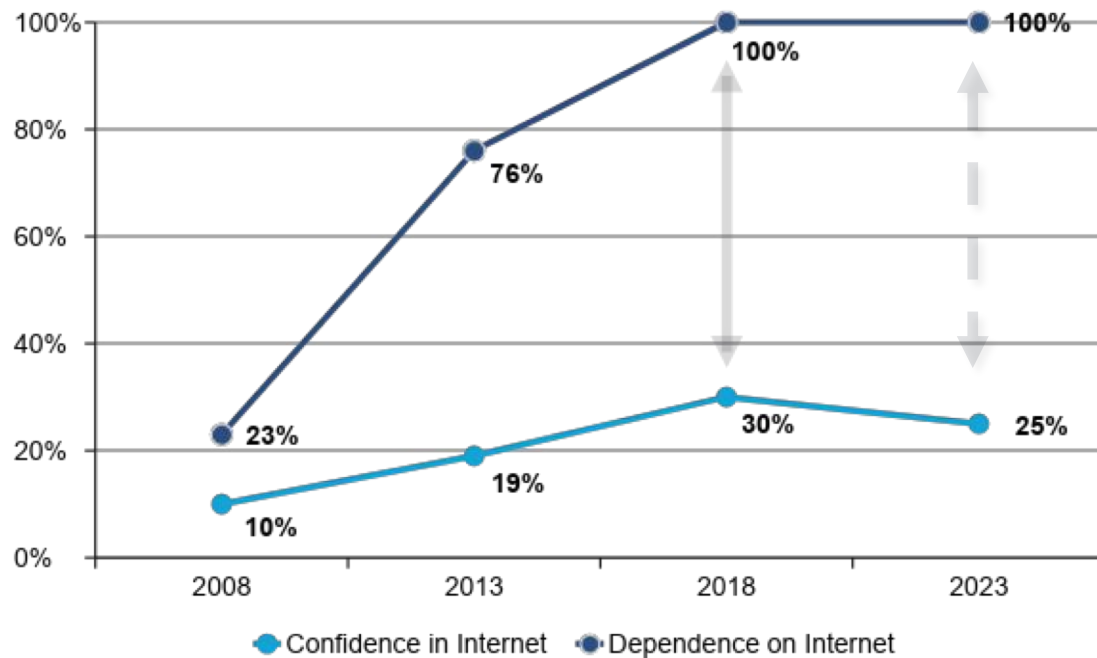
REUTERS

Exclusive: China hacked HPE, IBM and then attacked clients - sources

Wipro hacked & piggy-backed to target customers, highlights outsourcing risks

Equifax Says Cyberattack May Have Affected 143 Million in the U.S.

By Tara Siegel Bernard, Tiffany Hsu, Nicole Perlroth and Ron Lieber

Cybersecurity Confidence Is Low

Global CEOs Report:

Increased dependence on the Internet

Confidence in Internet security (already low at 30%) will drop even lower if nothing changes or improves

Cyber Risk Is Increasing

Cyber Incidents Are On The Rise

- Increasing in volume (number of attacks), speed, sophistication

The Targets Are Broad

- Your Own Organization
- Your Suppliers
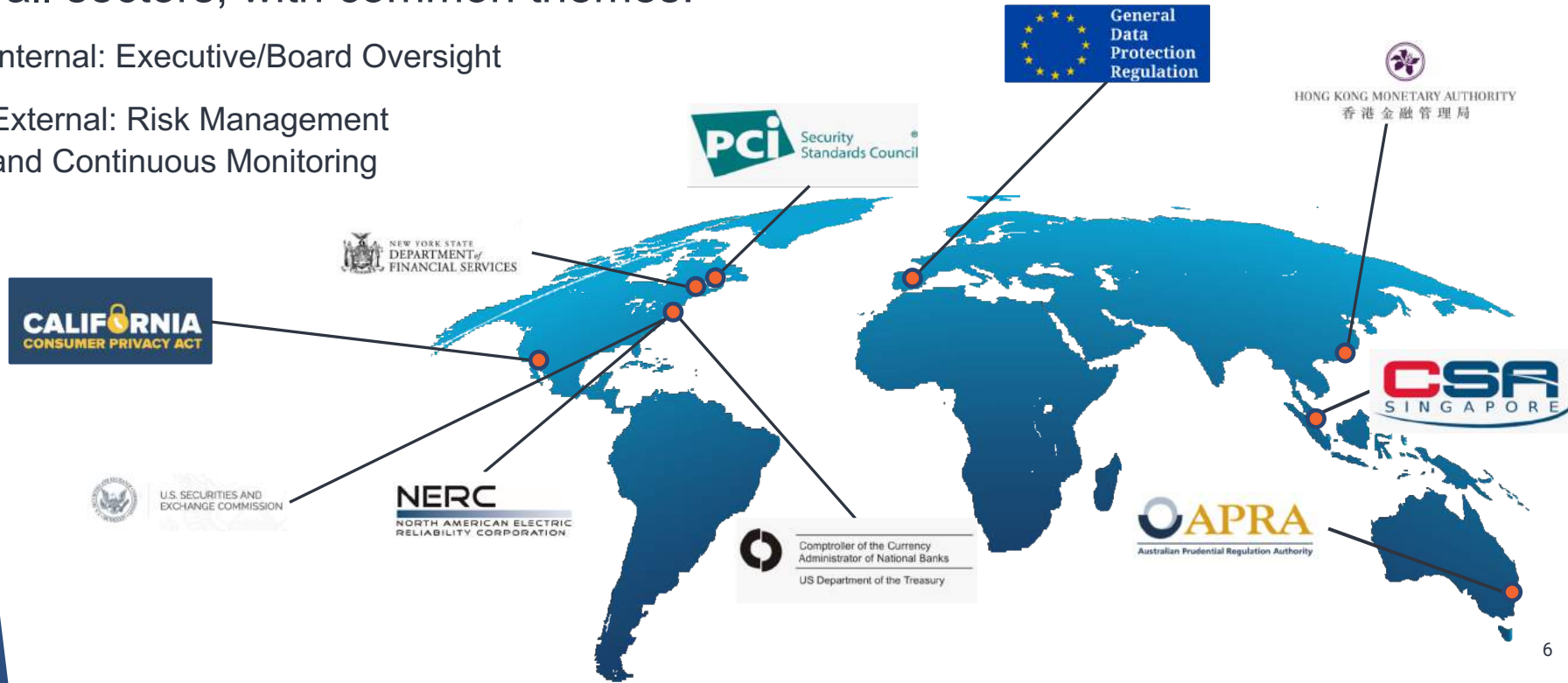- Your Customers

The Damage Is Severe

- Financial Loss
- Reputational Harm
- Legal Liability
- Operational Disruption

Global Regulators and Cybersecurity

New cyber requirements for companies in all sectors, with common themes:

- Internal: Executive/Board Oversight

- External: Risk Management and Continuous Monitoring

Mobile Software Facilitates the Spread of Botnets and Breaches

BitSight discovers and sinkholes about **one new malware family every other working day**.

In the last three months, BitSight has sinkholed **14 new mobile** malware families.

- *Ransomware; Trojan / RAT / Data theft; Ad fraud; App installer*

Performance grade vs Times more likely


Legend: Breaches, Botnet Infections
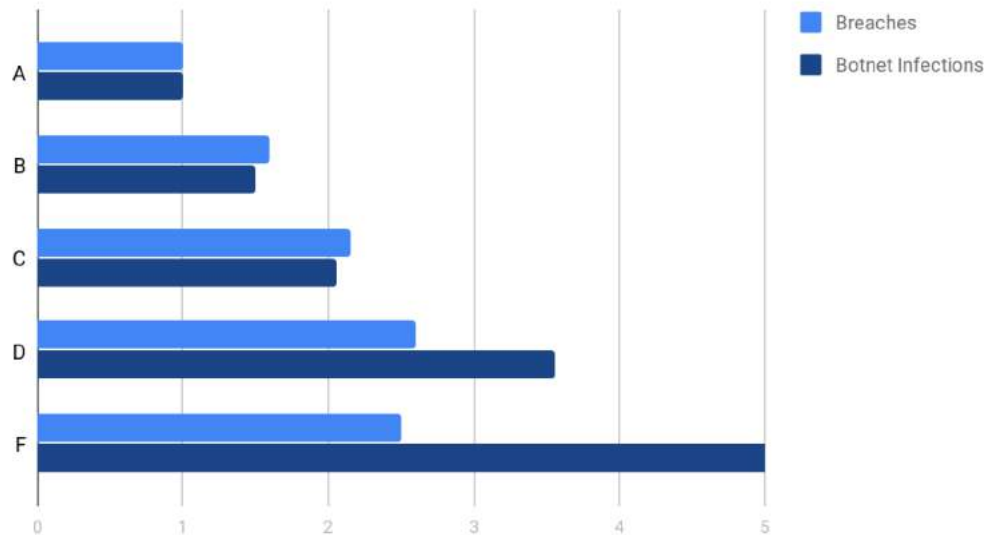
- Breaches involves both loss of data and loss of use

- Botnets are the most heavily weighted risk vector and have the greatest correlation to breach

"This vulnerability is pre-authentication and requires no user interaction. In other words, the vulnerability is 'wormable', meaning that any future malware that exploits this vulnerability could propagate from vulnerable computer to vulnerable computer in a similar way as the WannaCry malware spread across the globe in 2017."

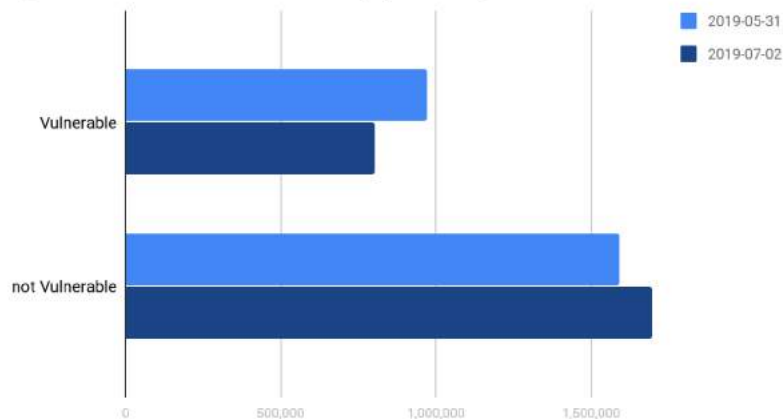- Microsoft Security Response Center, May 14, 2019
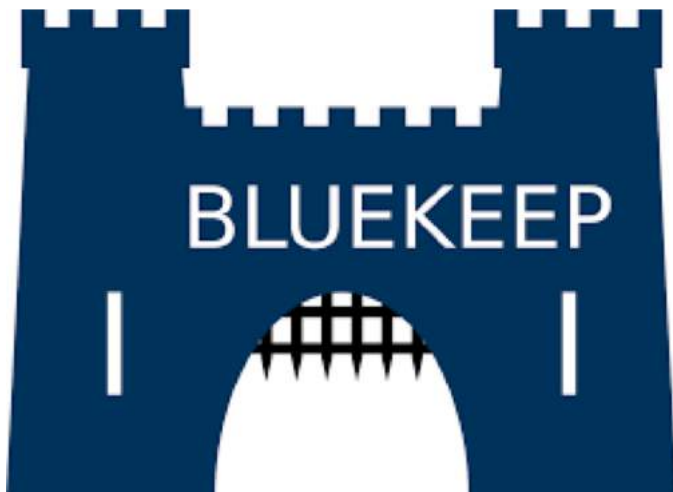
BlueKeep: Deep Visibility Into the Latest Threats

Goal: Quickly identify and gain visibility into the latest vulnerabilities and verify controls assurance

Actions by BitSight

Results

Global BlueKeep Analysis

Systems Vulnerable to Blue Keep (IP Count)

| | 2019-05-31 |
| | 2019-07-02 |

Vulnerable

not Vulnerable

0   500,000   1,000,000   1,500,000

"When BlueKeep came out, we **got notification from the CERT before it had widely hit the news**. At that time we issued a rapid response ticket to our teams globally. I**n a day or two all had reported that patches were applied**. I then looked in BitSight and found that we **still had BlueKeep vulnerabilities at our location in China (who had reportedly patched)**. I showed them the data, **they admitted they had missed some patches** and fixed the issue."

-- CISO of Large Global Manufacturer

BlueKeep: Median Security Rating of Vulnerable and Remediated Companies by Industry
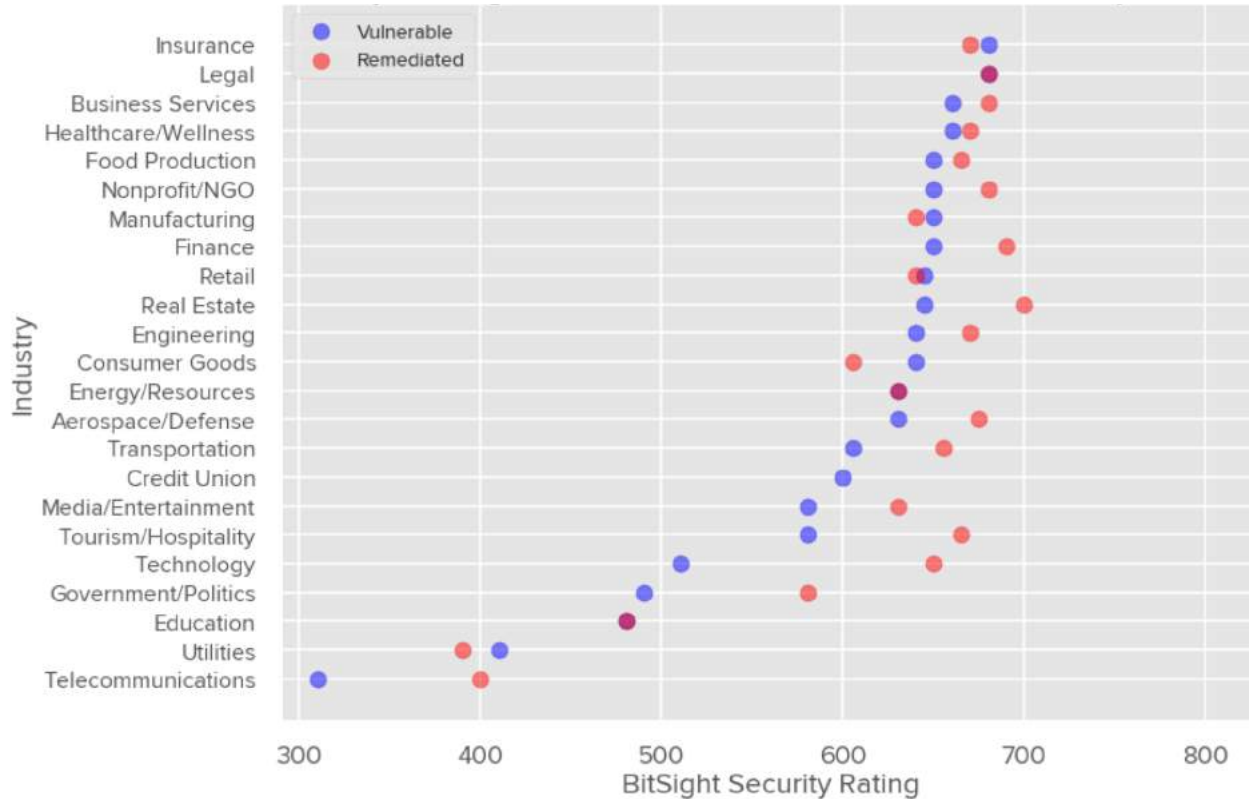
Future of Underwriting and Loss Control

Underwriting Scenario
Pre-binding Due Diligence

"We rejected the applicant because of the level of machine compromise" ~ Large Global Insurer

Loss Control Scenario
Post-bind Proactive Outreach

THE WALL STREET JOURNAL.

Home   World   U.S.   Politics   Economy   **Business**   Tech   Markets   Opinion   Life & Arts   Real Estate

CIO JOURNAL

Insurer Warns Client of Possible Breach

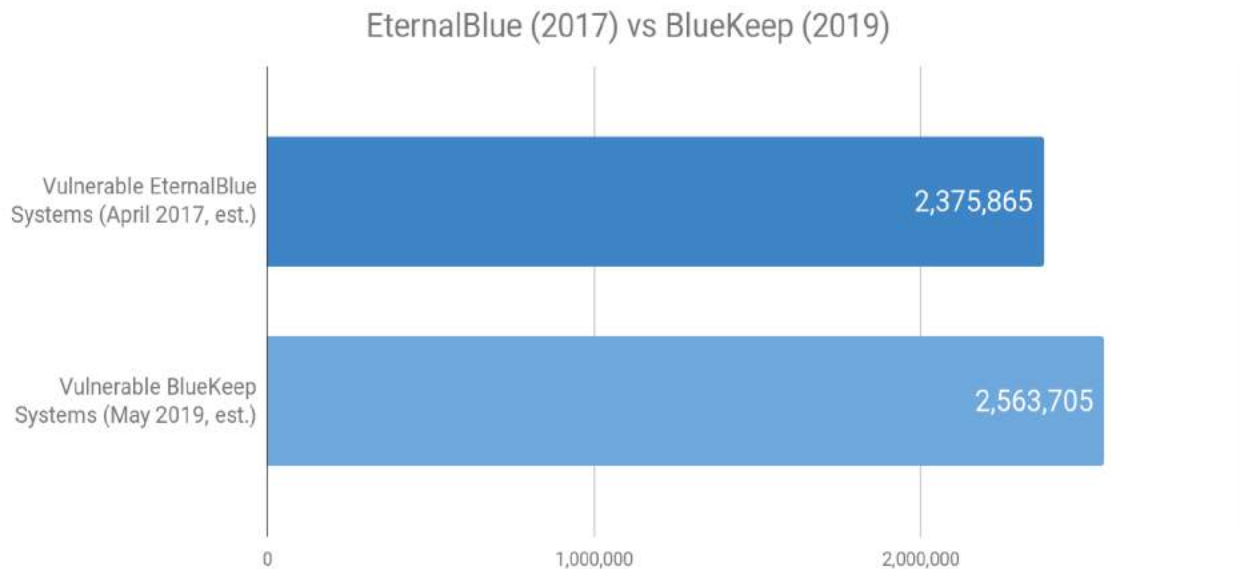*By Michael Hickins*   0 RESPONSES
Mar 11, 2014 6:05 pm ET

"Liberty International Underwriters ... uses BitSight Technologies Inc. **to monitor the networks of its clients**"

"According to Oliver Brew, vice president of privacy and technology at LIU, the **technology helped identify "a threat that had been dormant in their network for some time and helped them minimize that threat.**"

He added that the company "**had not yet suffered losses as a result of the threat**."

Future Losses? Learning From the Past...

According to estimates, WannaCry cost between $4B - $8B globally.

EternalBlue (2017) vs BlueKeep (2019)

Vulnerable EternalBlue Systems (April 2017, est.) — 2,375,865

Vulnerable BlueKeep Systems (May 2019, est.) — 2,563,705

0 | 1,000,000 | 2,000,000

We must build reliable models across sectors and companies to calculate financial impact from future cyber events.