



New York Oracle Users Group, Inc.

The Next Breach Target and How Oracle can help

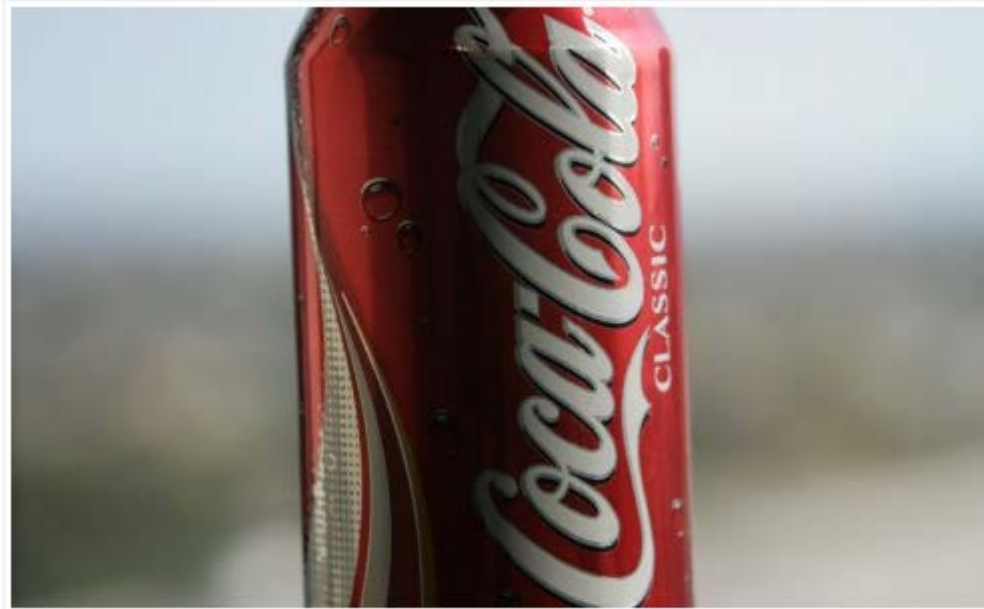
Ulf Mattsson
CTO, Protegrity

Ulf.Mattsson AT protegrity.com

Ulf Mattsson & PCI Data Security Standards

Working in Task Forces at Payment Card Industry Security Standards Council (PCI SSC):

1. PCI SSC Tokenization Task Force
2. PCI SSC Encryption Task Force
3. PCI SSC Point to Point Encryption Task Force
4. PCI SSC Risk Assessment SIG
5. PCI SSC eCommerce SIG
6. PCI SSC Cloud SIG
7. PCI SSC Virtualization SIG
8. PCI SSC Pre-Authorization SIG
9. PCI SSC Scoping SIG Working Group 2
10. PCI SSC 2013 – 2014 Tokenization Task Force (TkTF)



Mary Ann Davidson, Chief Security Officer, Oracle Corporation



Is the Cloud the Answer? What Coke's Recent Breach Teaches Us

Scott Walters March 10, 2014 No Comments »



Coke recently disclosed that sensitive information belonging to approximately 70,000 current and former North American employees was compromised because the data hadn't been encrypted on company laptops (despite the company's encryption policy).[1] The data breach occurred after a former worker stole several company laptops that locally stored employee information, such as Social Security and driver's license numbers.

Target Data Breach, U.S. Secret Service & iSIGHT



Target CIO
Beth Jacob
resigned

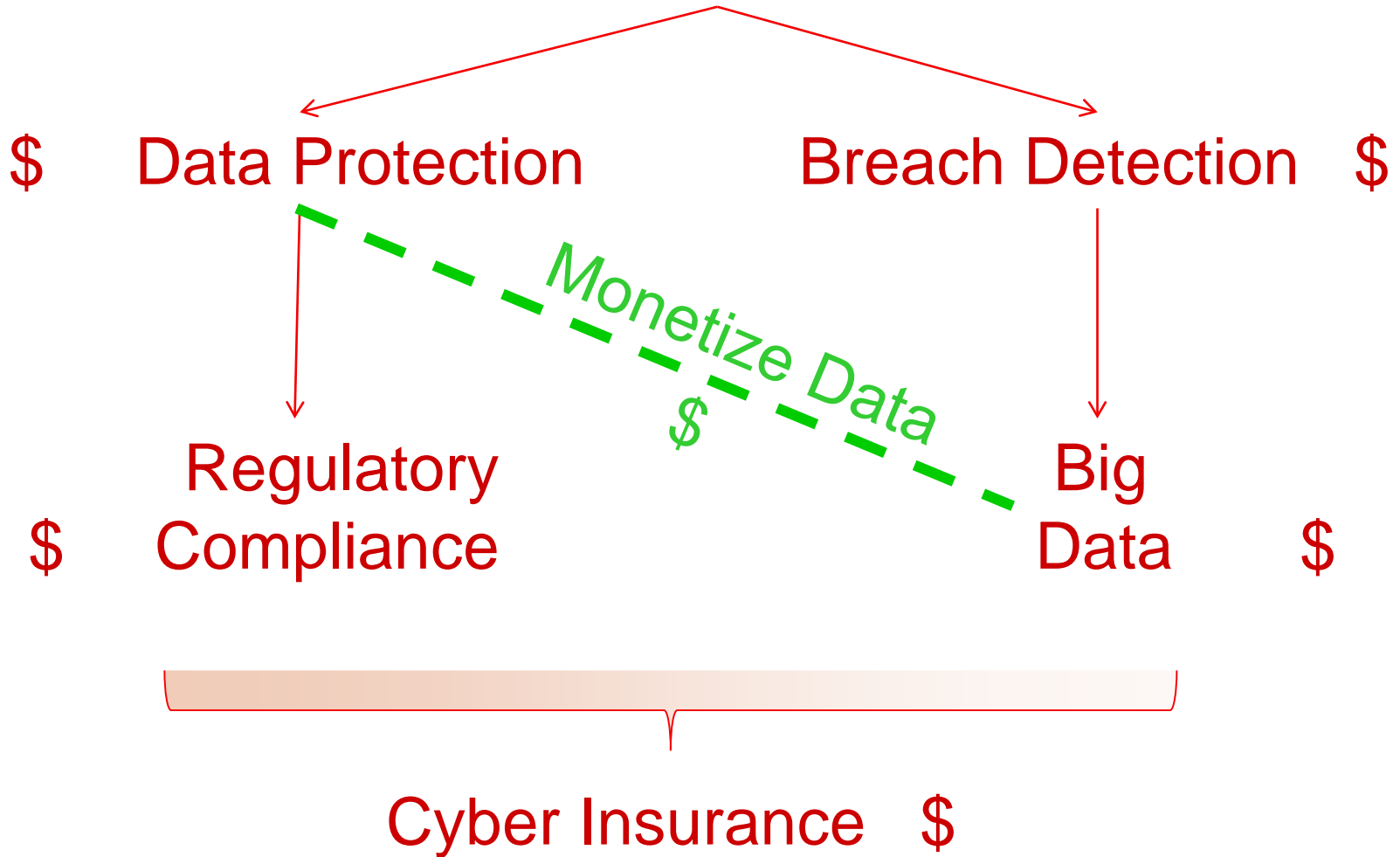


POS Malware Technical Analysis: Indicators for Network Defenders

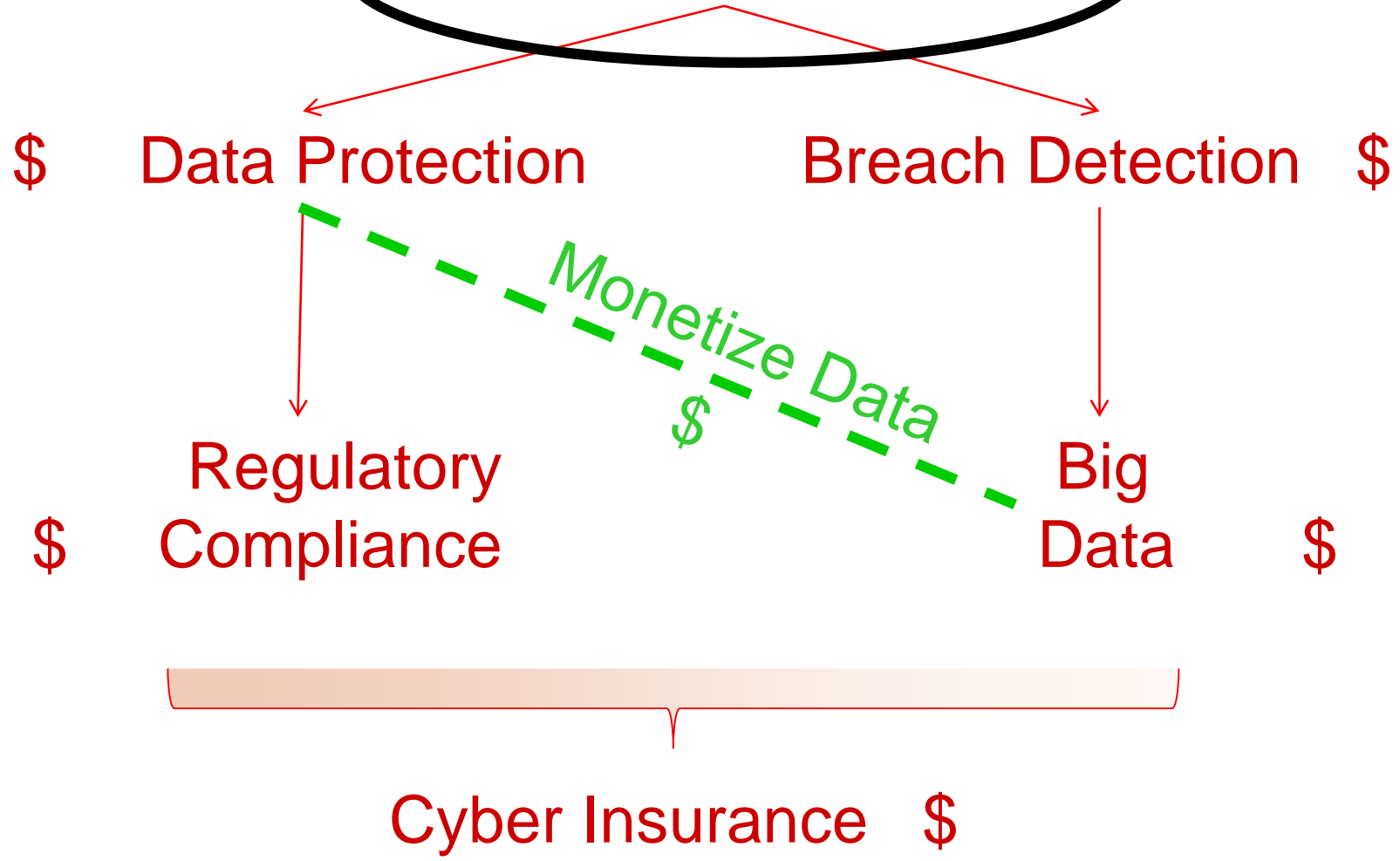
Jan. 17, 2014



Threat Landscape



Threat Landscape



THE CHANGING THREAT LANDSCAPE

How have the methods of attack shifted?

The 2014 Verizon Data Breach Investigations Report

It's clear the bad guys are winning at a faster rate than the good guys are winning, and we've got to solve that.

Wade Baker,
managing principal
for research and
intelligence, Verizon

The report will include first-time contributions from not only a number of national and international computer emergency response teams, such as [CERT Polska](#) and others from Eastern Europe and Latin America, but also from well-known commercial security vendors, including McAfee Inc. and FireEye Inc., companies that are fierce rivals in most circumstances but are coming together to support Verizon's breach-analysis efforts.

The [2013 DBIR](#) set a record by incorporating breach incident data from Verizon and 18 other organizations around the world; last year's first-time contributors included the U.S. Computer Emergency Readiness Team (US-CERT) and the

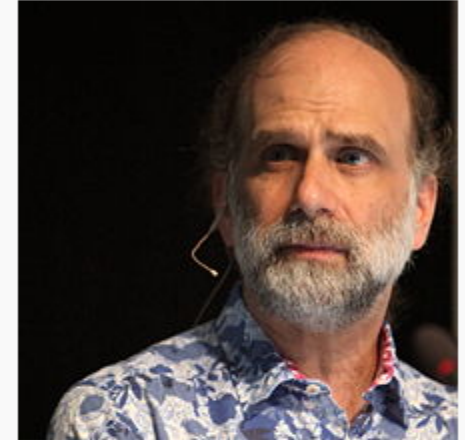
The 2014 DBIR is expected to be released this spring

Security Improving but We Are Losing Ground



1

Bruce Schneier



Bruce Schneier at the Congress on Privacy & Surveillance (2013) of the *École polytechnique fédérale de Lausanne (EPFL)*.

Born	January 15, 1963 (age 50) ^[1] New York City, New York
Residence	United States
Citizenship	American
Fields	Computer science
Institutions	Counterpane Internet Security Bell Labs United States Department of Defense BT Group
Alma mater	American University University of Rochester
Known for	Cryptography, security



Cloud, Virtualization Drive Enterprise Network Complexity

By Nathan Eddy | Posted 2013-10-31



IT professionals and C-level executives are tackling increasingly complex enterprise networks, with trends such as virtualization, Internet Protocol version 6 (IPv6) and the cloud requiring more automation of network management, according to a survey of more than 500 IT professionals in the United States and United Kingdom by security specialist Tufin Technologies.

One-third (33 percent) of U.K. and U.S. IT and business decision-makers said their companies had suffered five or more firewall-related outages in the last year—the equivalent of nearly one every other month, with 17 percent of financial services companies reporting 11 or more outages in the last 12 months.

The survey indicated that human error is a common security issue, with one-quarter of U.K. and U.S. businesses having to re-do more than 60 percent of all firewall changes because they weren't implemented correctly the first time.

Business Insider: Are people at more risk from computer crime today than, say, a decade ago?

Bruce Schneier: Sure. That's obvious. There are more people using computers.

BI: But a decade ago, we were running Windows XP and there have been a whole lot of security developments since then. Have none of these worked?

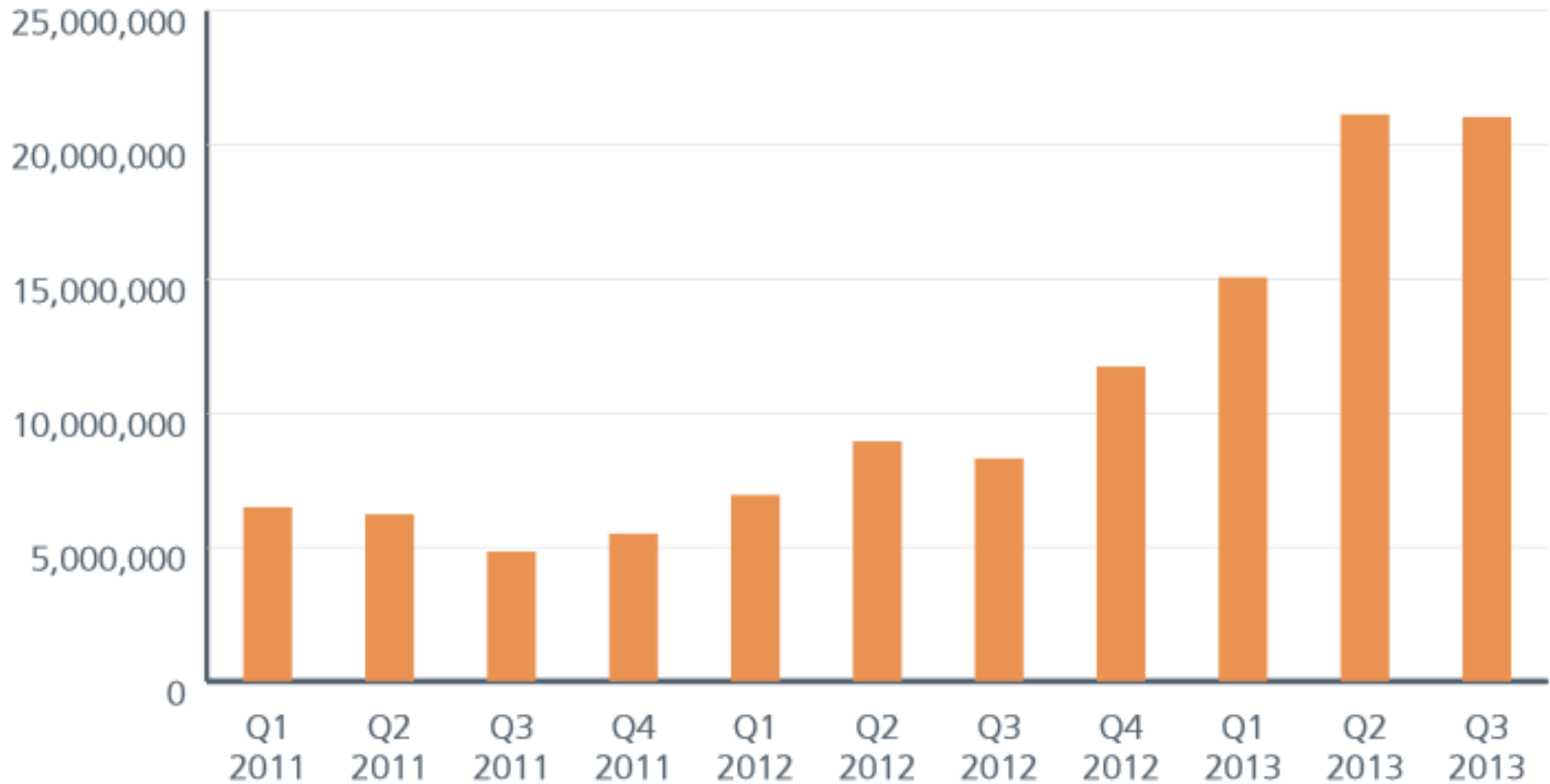
BS: It doesn't matter if they've worked. Things are getting more secure faster. So yes. The new version of Windows is better than XP. It's more secure. On the other hand, there are 10 times more people out there with computers and they are doing more online. So even though security is improving, things are getting worse faster, so we're losing ground even as we improve.

The Biggest Cyber Attack Detected in Feb 2014

- 360 million email accounts
- 1.25 billion email addresses without passwords
- 105 million records were stolen in a single data breach
- The email addresses came from
 - All the major providers, including Google, Microsoft and Yahoo.
 - Non-profit organizations
 - Almost all Fortune 500 companies were affected by the attacks
 - Some have not made their security breaches public

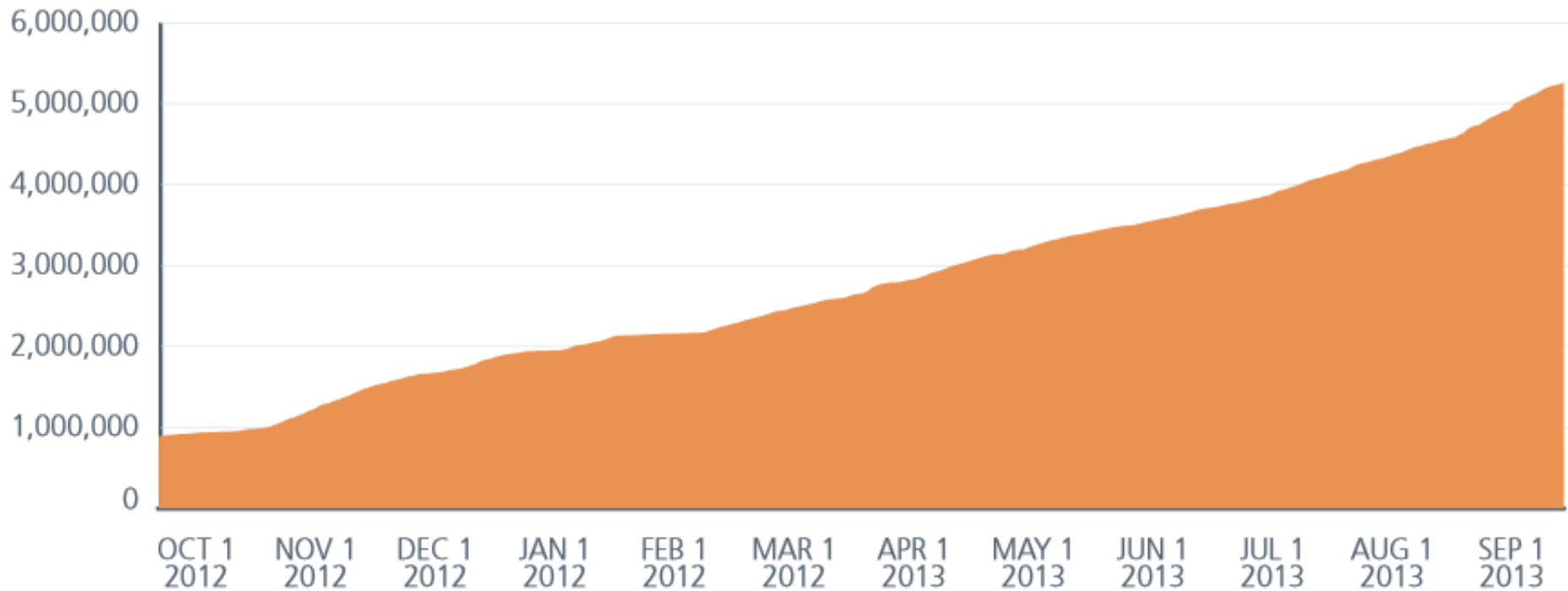
According to the cybersecurity firm Hold Security LLC

New Malware



Source: mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf

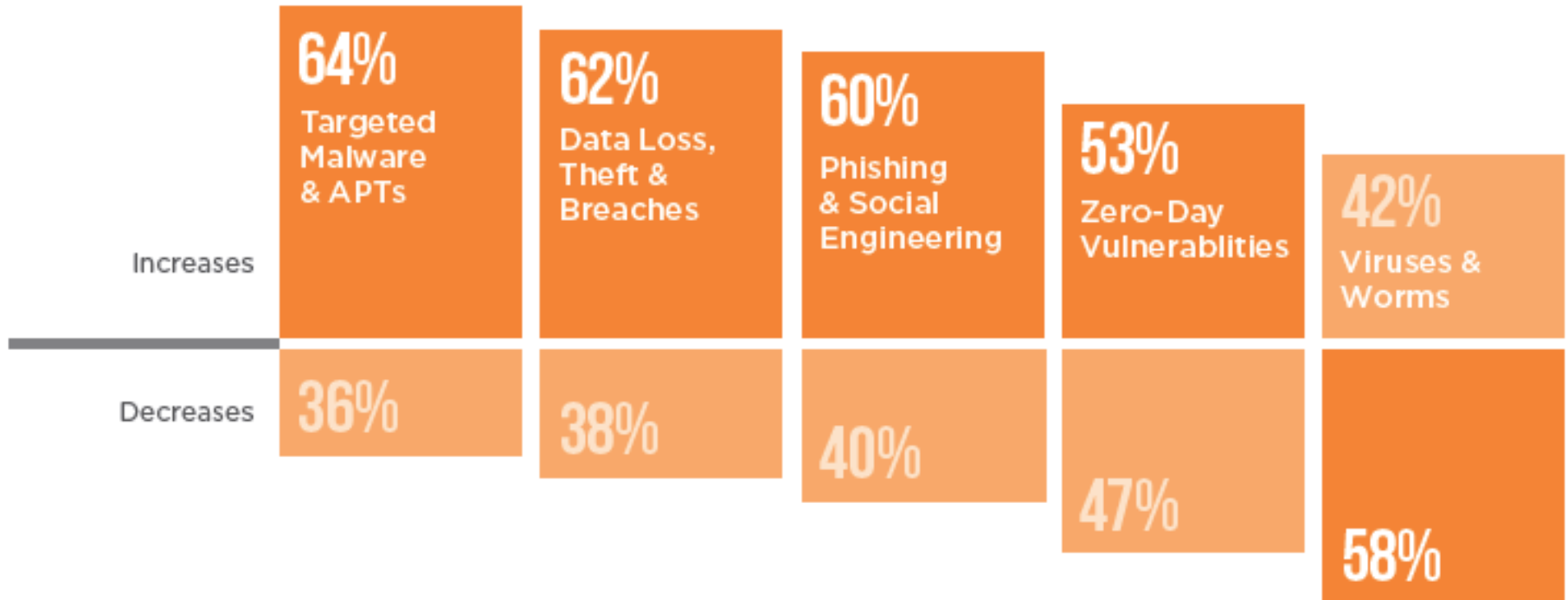
Total Malicious Signed Malware



Source: mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2013.pdf

Targeted Malware Topped the Threats

Security Threats Result in Pressure



62% said that the pressure to protect from data breaches also increased over the past year.

Source: 2014 Trustwave Security Pressures Report

US and Canada - Targeted Malware Top Threat

Increased Pressures to Protect from...

	United States	Canada	United Kingdom	Germany	Overall
Targeted Malware & APTs	68%	63%	62%	48%	64%
Data Loss, Theft & Breaches	67%	51%	42%	51%	62%
Phishing & Social Engineering	60%	58%	64%	60%	60%
Zero-Day Vulnerabilities	59%	47%	45%	35%	53%
Viruses & Worms	49%	36%	30%	34%	42%

In the United States and Canada, targeted malware was the top threat IT pros felt pressured to secure against, and in the U.K. and Germany, the top threat was phishing/social engineering. Respondents in each country surveyed said viruses and worms caused the lowest pressure.

Source: 2014 Trustwave Security Pressures Report

Fallout – FBI Memory-Scraping Malware Warning

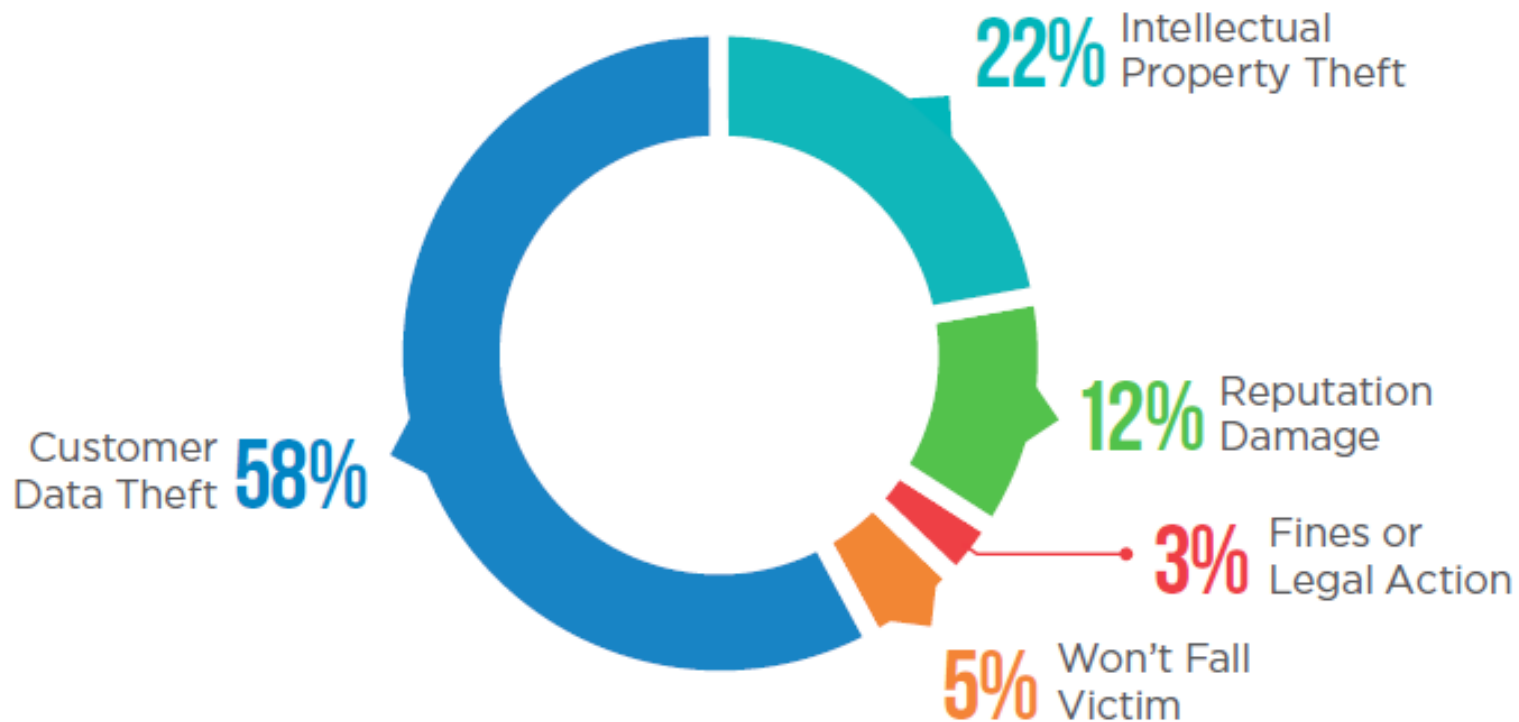
Report: *“Recent Cyber Intrusion Events Directed Toward Retail Firms”*

- FBI uncovered 20 cyber attacks against retailers in the past year that utilized methods similar to Target incident
- "We believe POS malware crime will continue to grow over the near term, despite law enforcement and security firms' actions to mitigate it."

Source: searchsecurity.techtarget.com/news/2240213143/FBI-warns-of-memory-scraping-malware-in-wake-of-Target-breach

Data Loss Worries IT Pros Most

Top Cyberattack and Data Breach Worries



Source: 2014 Trustwave Security Pressures Report

Energy Sector a Prime Target for Cyber Attacks

- July 2012 - June 2013: 74 targeted cyber attacks/day
 - #1: Government/Public sector – 25.4%
 - #2: Energy sector - 16.3%
- Oct. 2012 - May 2013: The U.S. government's Industrial Control Systems Cyber Emergency Response Team responded to more than 200 incidents — 53% aimed at the energy sector.
- So far, there have not been any successful catastrophic attacks on the US energy grid, but there is ongoing debate about the risk of a "cyber Pearl Harbor" attack.

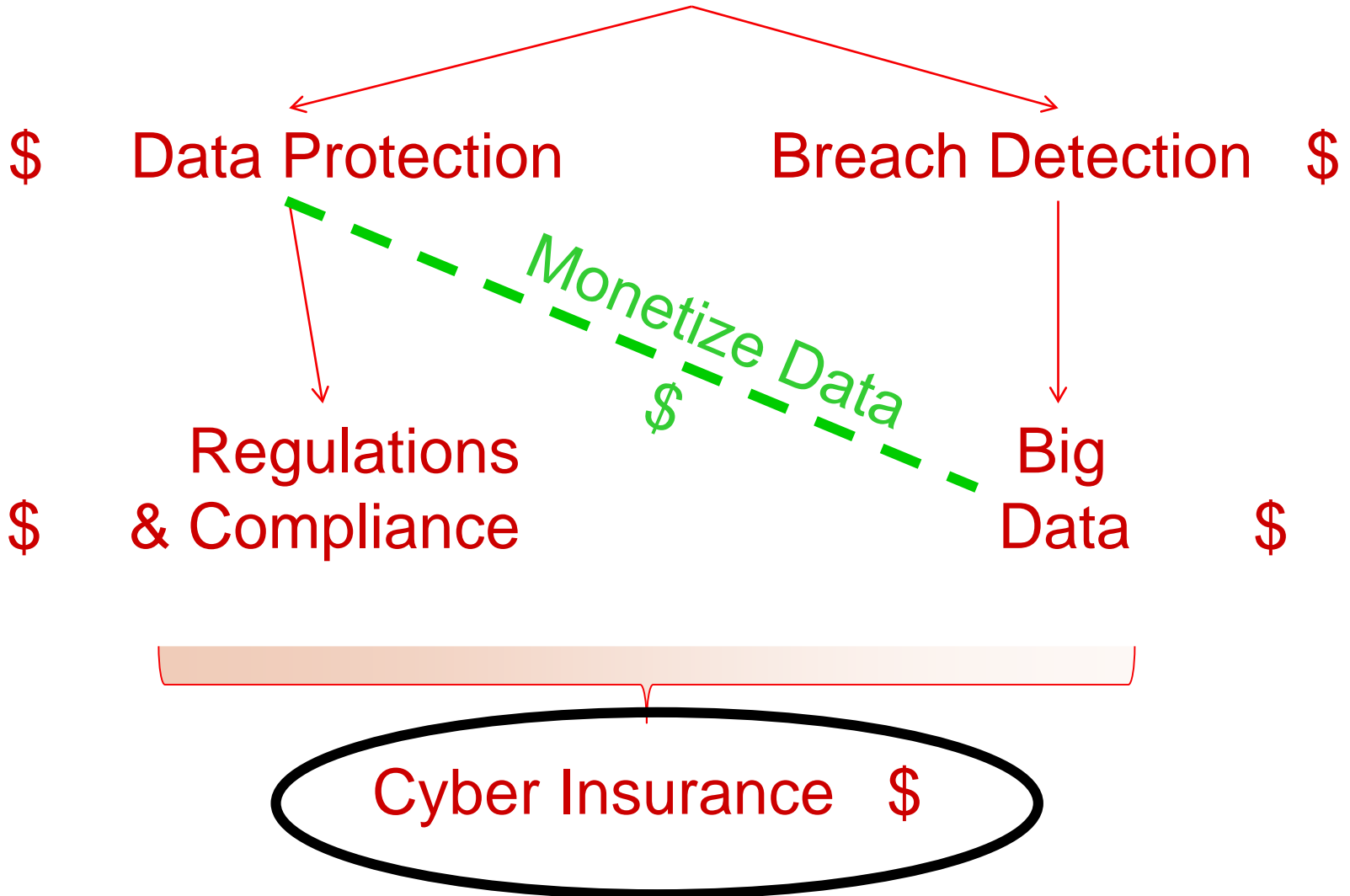
Source: www.csoonline.com/article/748580/energy-sector-a-prime-target-for-cyber-attacks

UK Energy Companies Refused Insurance



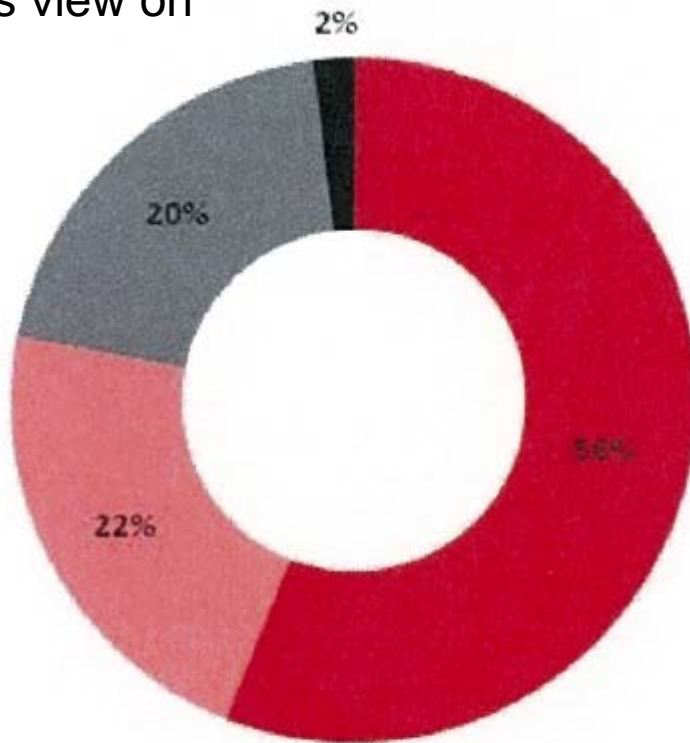
www.itproportal.com/2014/02/27/uk-energy-companies-refused-insurance-due-to-inadequate-cyber-defences/#ixzz2ud7g2hmO

Threat Landscape

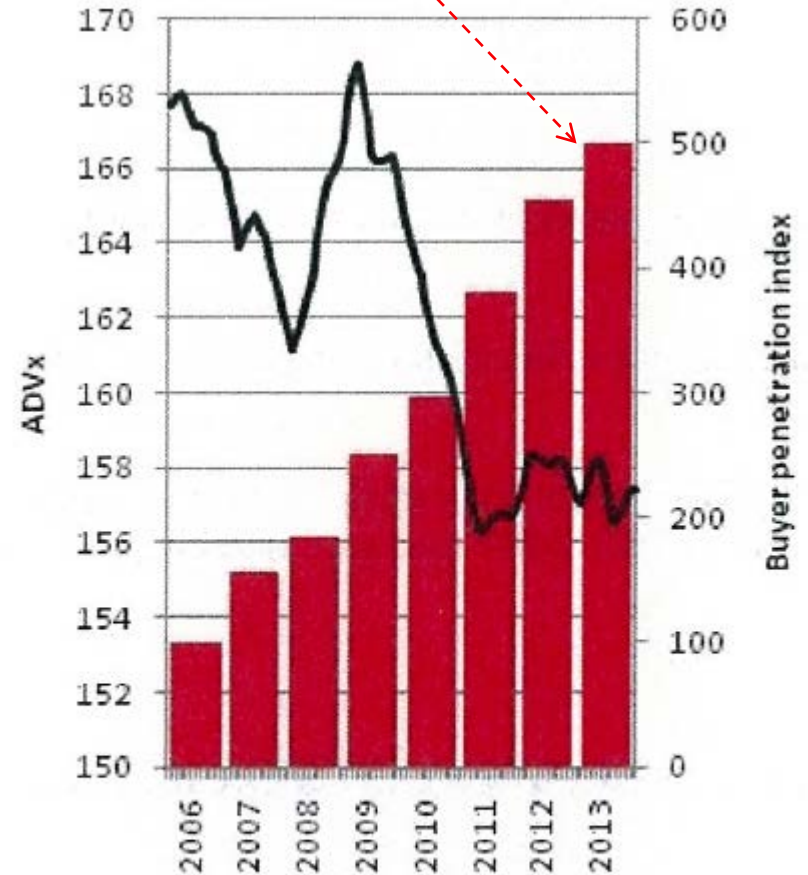
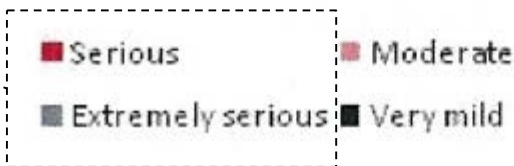


Cyber Insurance Increases 5x Globally

Companies view on cyber risk



76%
(up 19%)



■ The popularity of cyber insurance (Buyer Penetration Index)
— The price of cyber insurance (ADVx index)



Cyber Attacks are a Real and Growing Threat

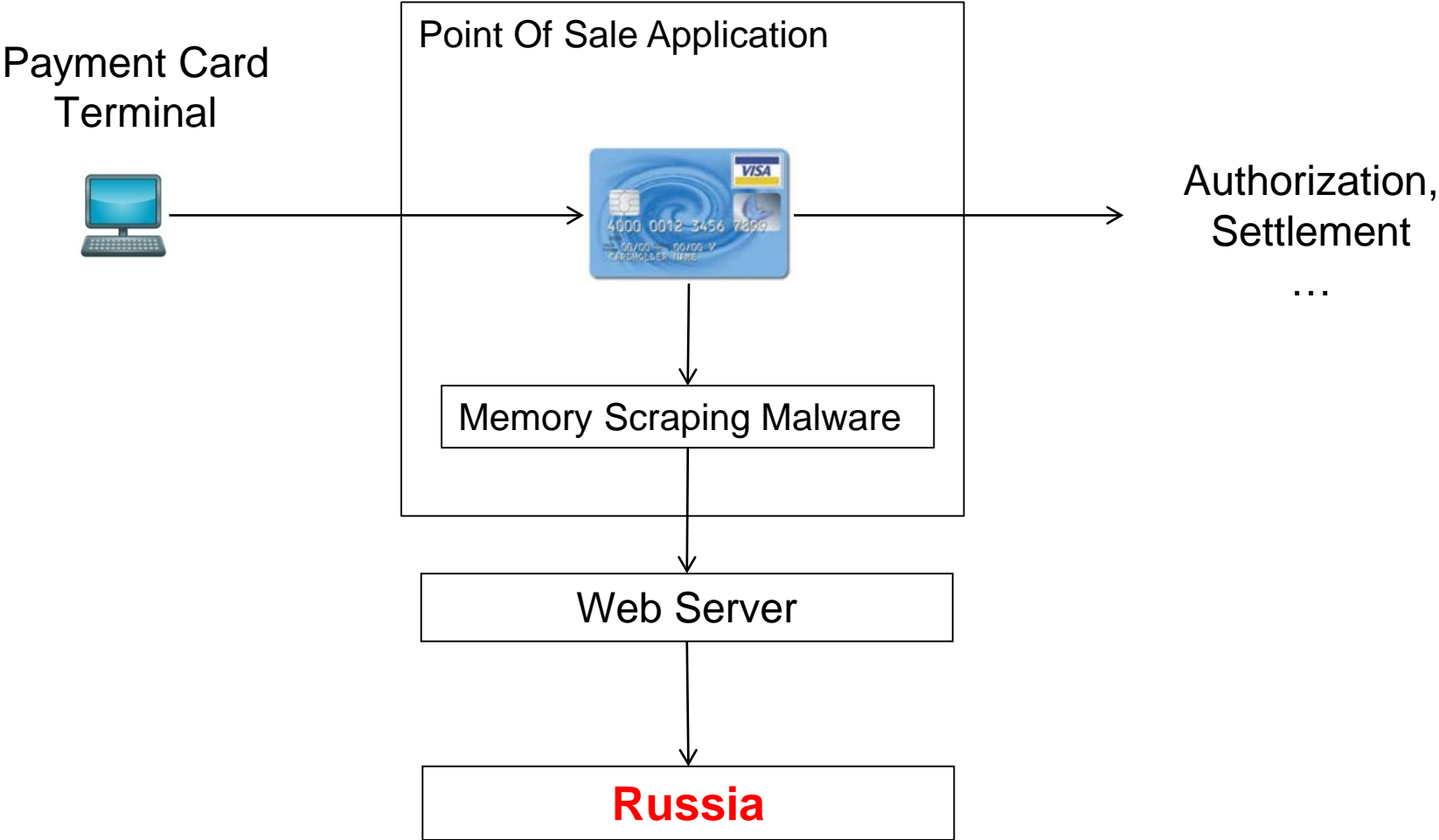
- Organizations worldwide are not "sufficiently protected" against cyber attack
- Cyber attack fallout could cost the global economy \$3 trillion by 2020
- The report states that if "attackers continue to get better more quickly than defenders," as is presently the case, "this could result in a world where a 'cyberbacklash' decelerates digitization."

Source: McKinsey report on enterprise IT security implications released in January 2014.

TARGET DATA BREACH

What can we learn from the Target breach?

Memory Scraping Malware – Target Breach



How The Breach at Target Went Down

- Credentials were stolen from Fazio Mechanical in a malware-injecting phishing attack sent to employees of the firm by email
 - Resulted in the theft of at least 40 million customer records containing financial data such as debit and credit card information.
 - In addition, roughly 70 million accounts were compromised that included addresses and mobile numbers.
- The data theft was caused by the installation of **malware** on the firm's point of sale machines
 - Free version of Malwarebytes Anti-Malware was used by Target
- The subsequent file dump containing customer data is reportedly flooding the black market
 - Starting point for the manufacture of fake bank cards, or provide data required for identity theft.

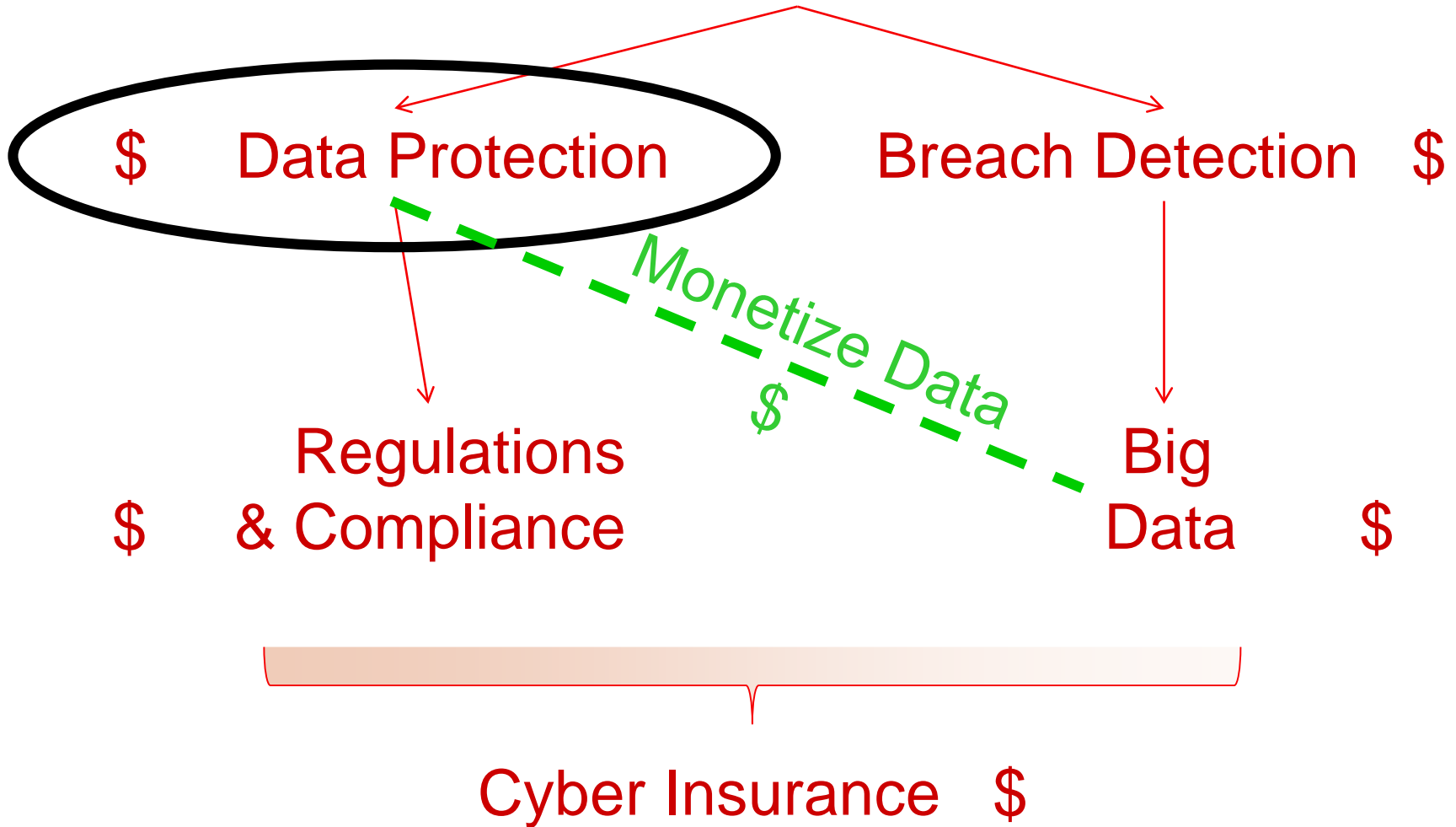
Source: Brian Krebs and www.zdnet.com/how-hackers-stole-millions-of-credit-card-records-from-target-7000026299/

It's not like other businesses are using some special network security practices that Target doesn't know about.

They just haven't been hit yet.

No number of traps, bars, or alarms will keep out the determined thief.

Threat Landscape



THINKING LIKE A HACKER

How can we shift from reactive to proactive thinking?

What if a
Social Security number or
Credit Card Number
in the Hands of a Criminal
was Useless?

TURNING THE TIDE

What new technologies and techniques can be used to prevent future attacks?

Evolution of Data Security Methods

○ Coarse Grained Security

- Access Controls
- Volume Encryption
- File Encryption

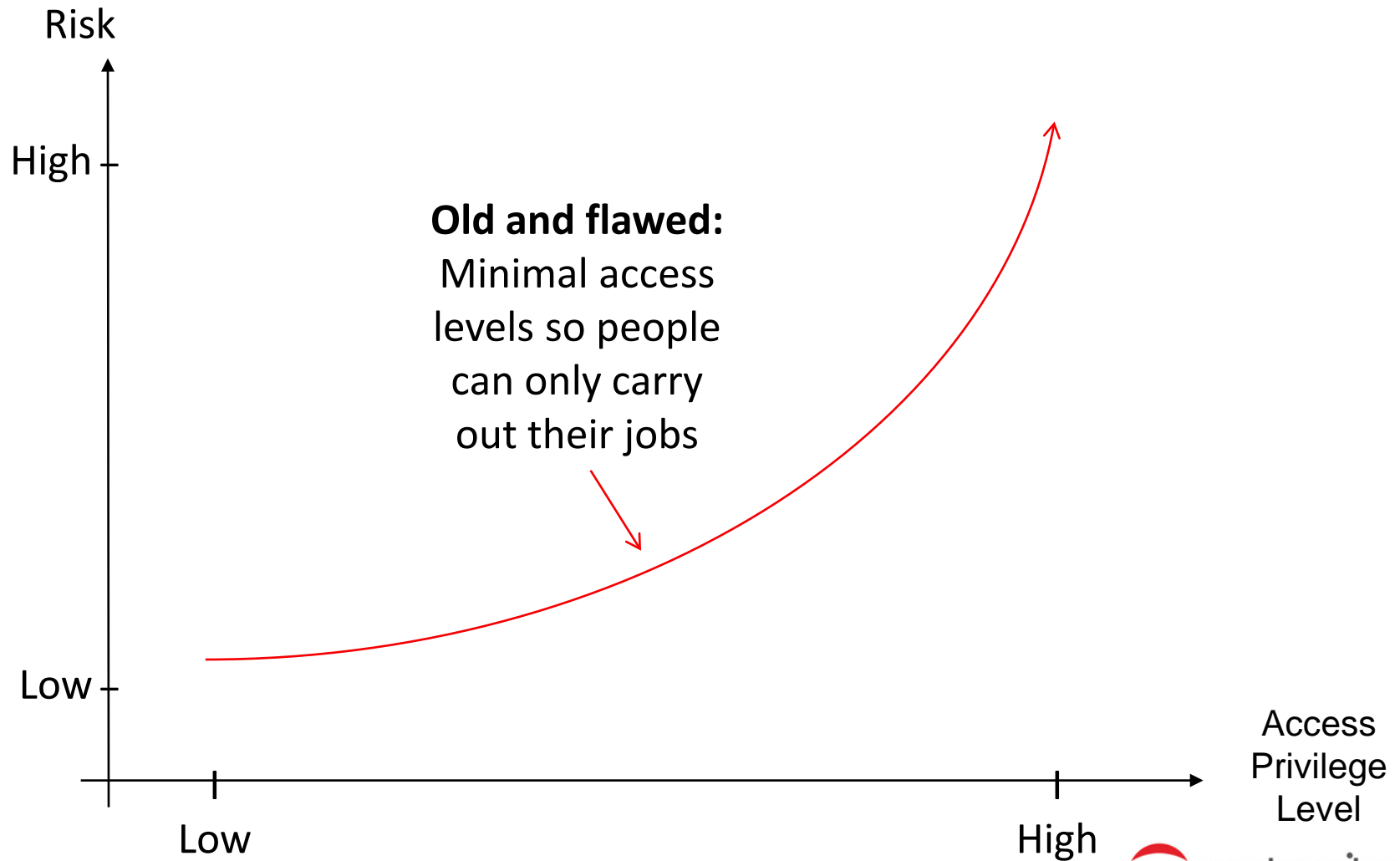
○ Fine Grained Security

- Access Controls
- Field Encryption (AES &)
- Masking
- Tokenization
- Vaultless Tokenization

Time

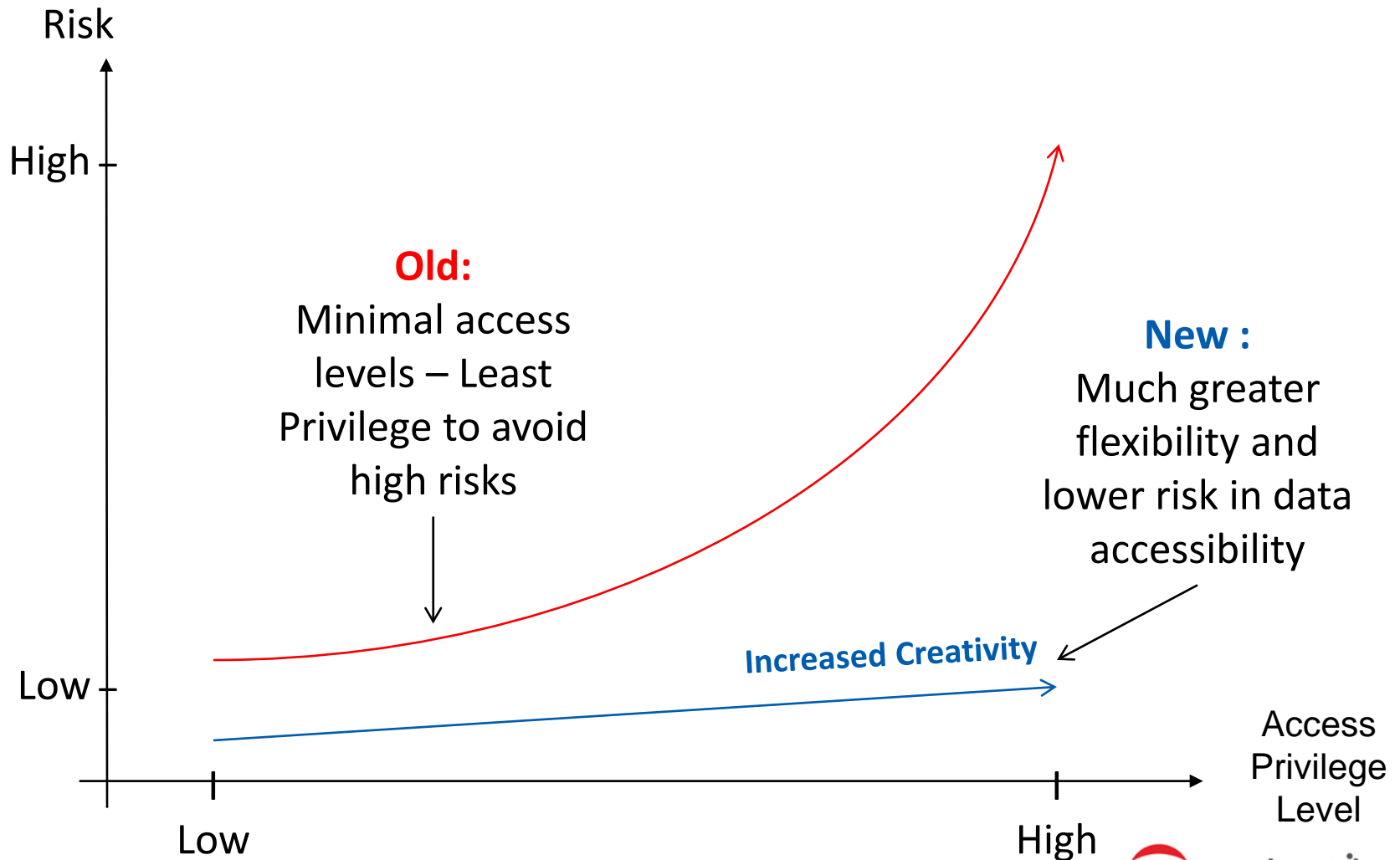


Access Control

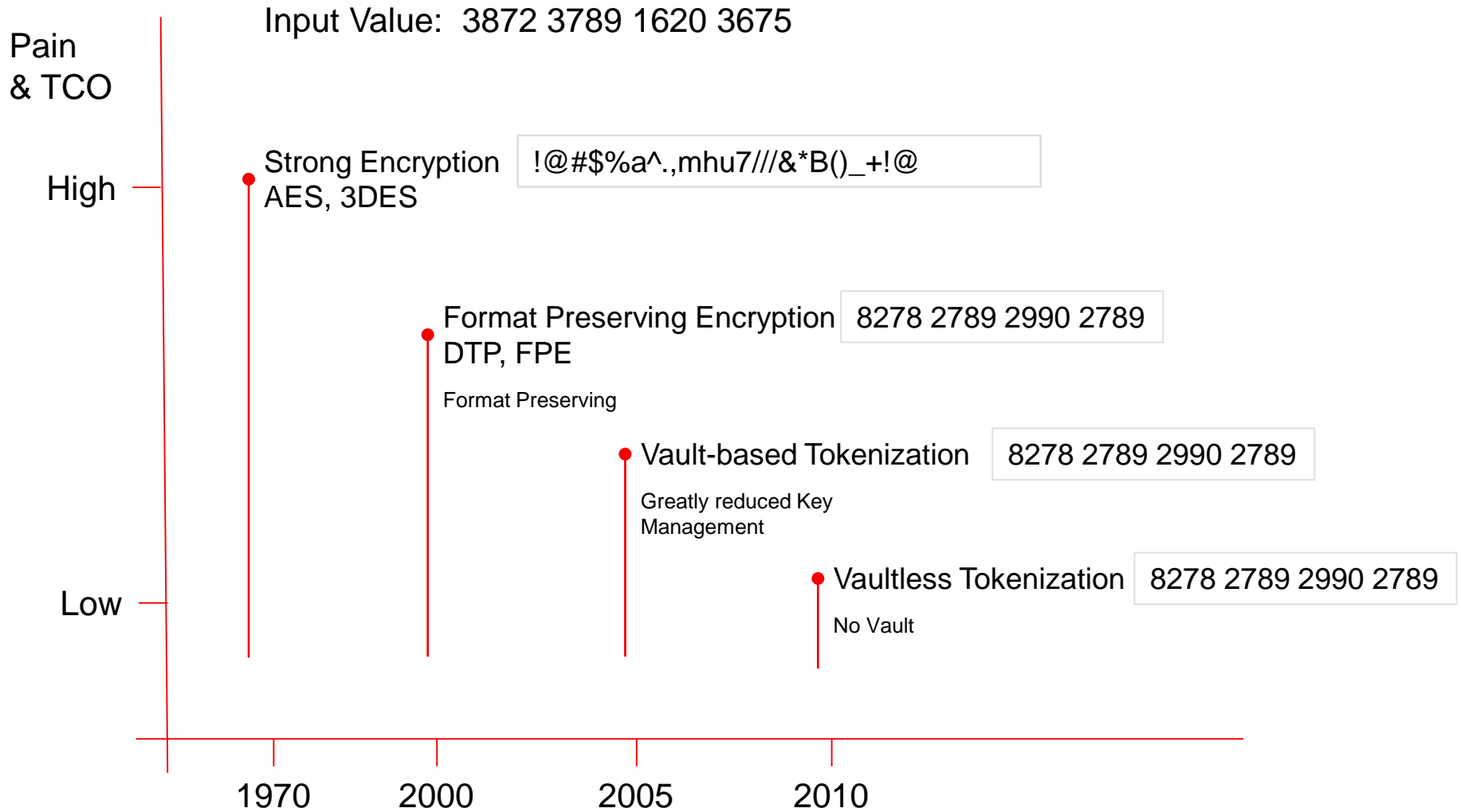


Applying the
Protection Profile to the
Structure of each
Sensitive Data Fields allows for
a Wider Range
of Granular Authority Options

The New Data Protection - Tokenization



Reduction of Pain with New Protection Techniques

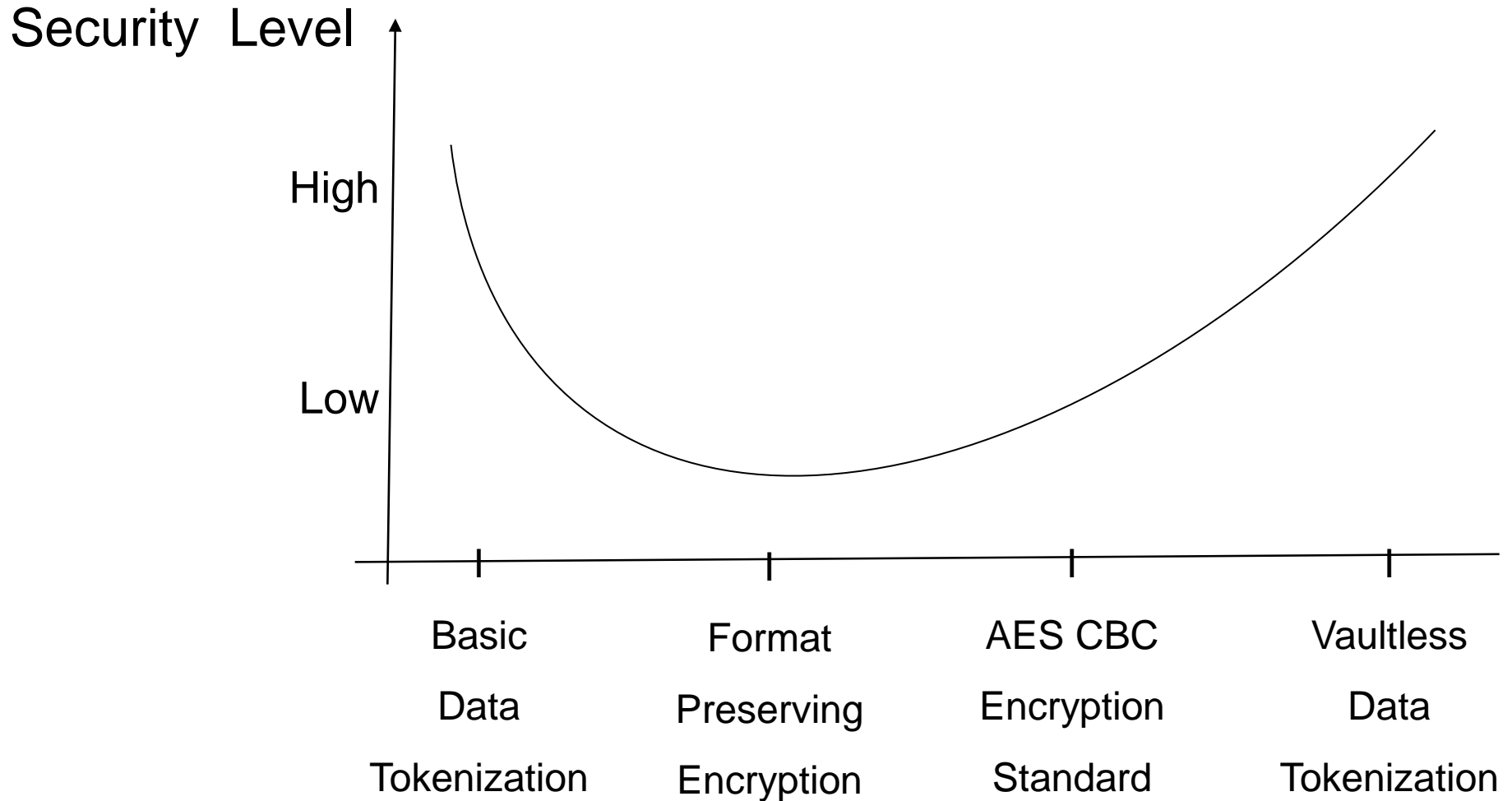


Tokenization Gets Traction

- Aberdeen has seen a steady increase in enterprise use of tokenization for protecting sensitive data over encryption
- Nearly half of the respondents (47%) are currently using tokenization for something other than cardholder data
- Over the last 12 months, tokenization users had 50% fewer security-related incidents than tokenization non-users

Source: <http://www.protegrity.com/2012/08/tokenization-gets-traction-from-aberdeen/>

Security of Different Protection Methods



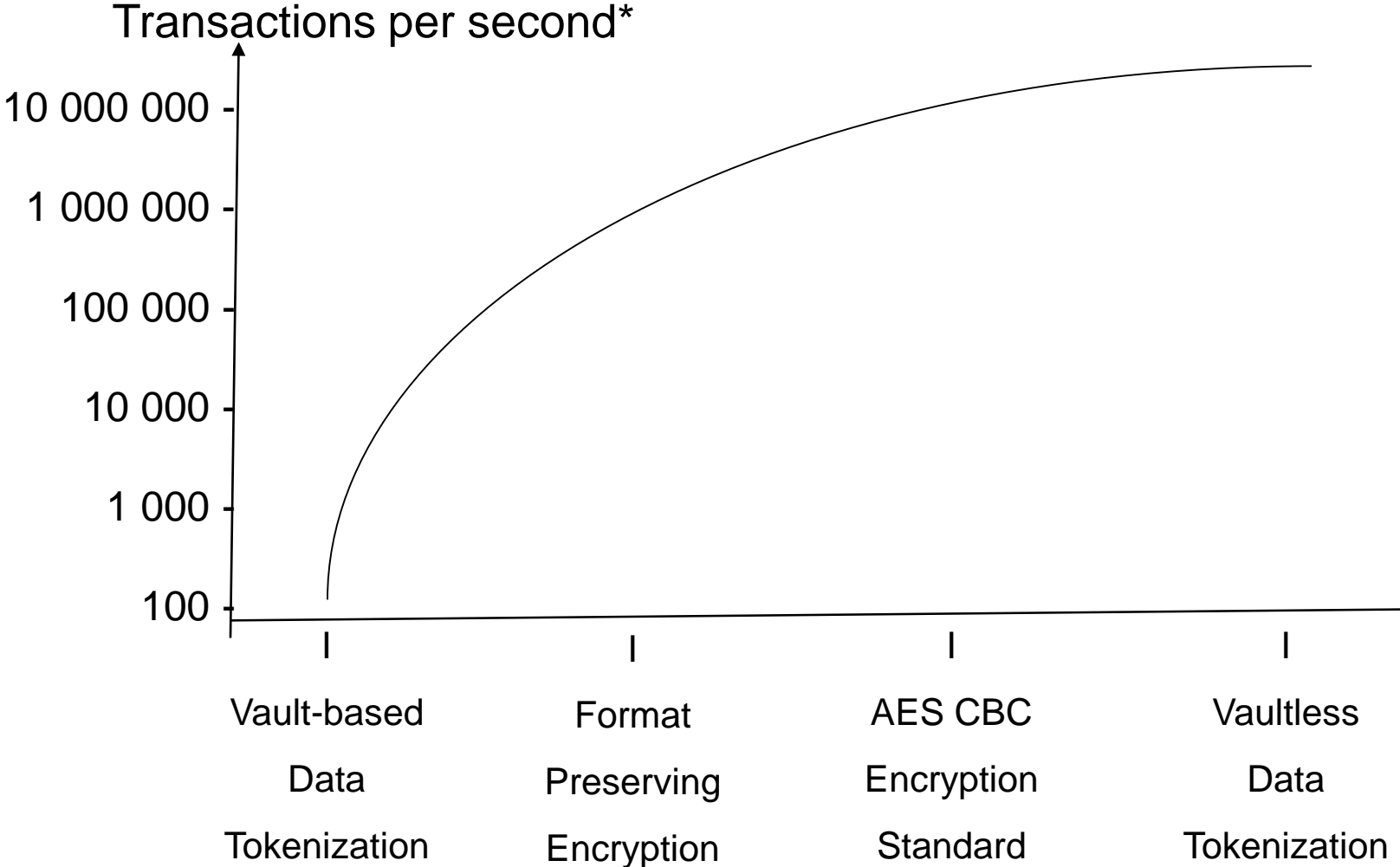
Fine Grained Data Security Methods

Tokenization and Encryption are Different

	Encryption	Tokenization
Used Approach	Cipher System	Code System
Cryptographic algorithms	●	
Cryptographic keys	●	
Code books		●
Index tokens		●

Source: McGraw-HILL ENCYCLOPEDIA OF SCIENCE & TECHNOLOGY

Speed of Different Protection Methods



*: Speed will depend on the configuration



Different Tokenization Approaches

Vault-based

Property

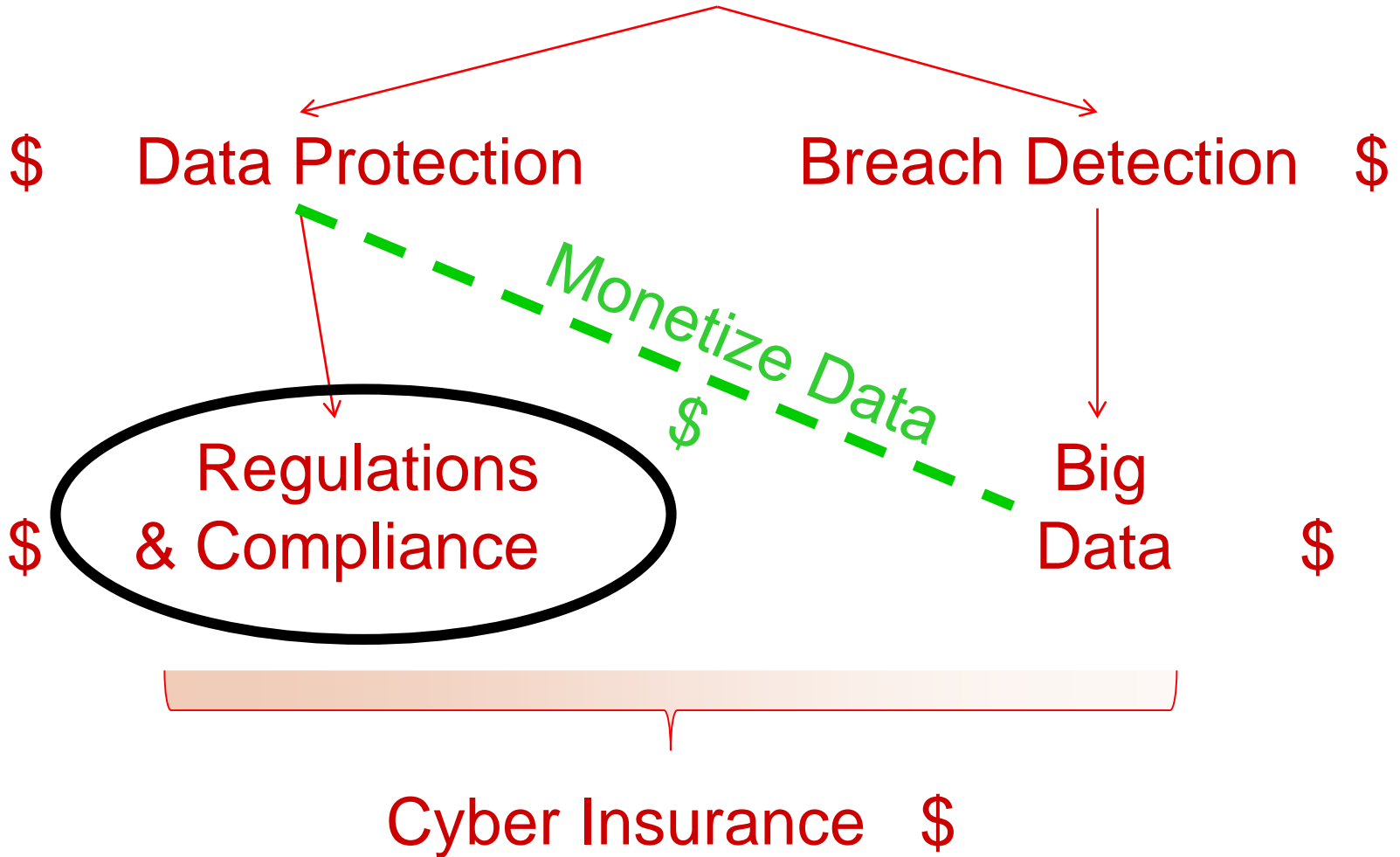
Dynamic

Pre-generated

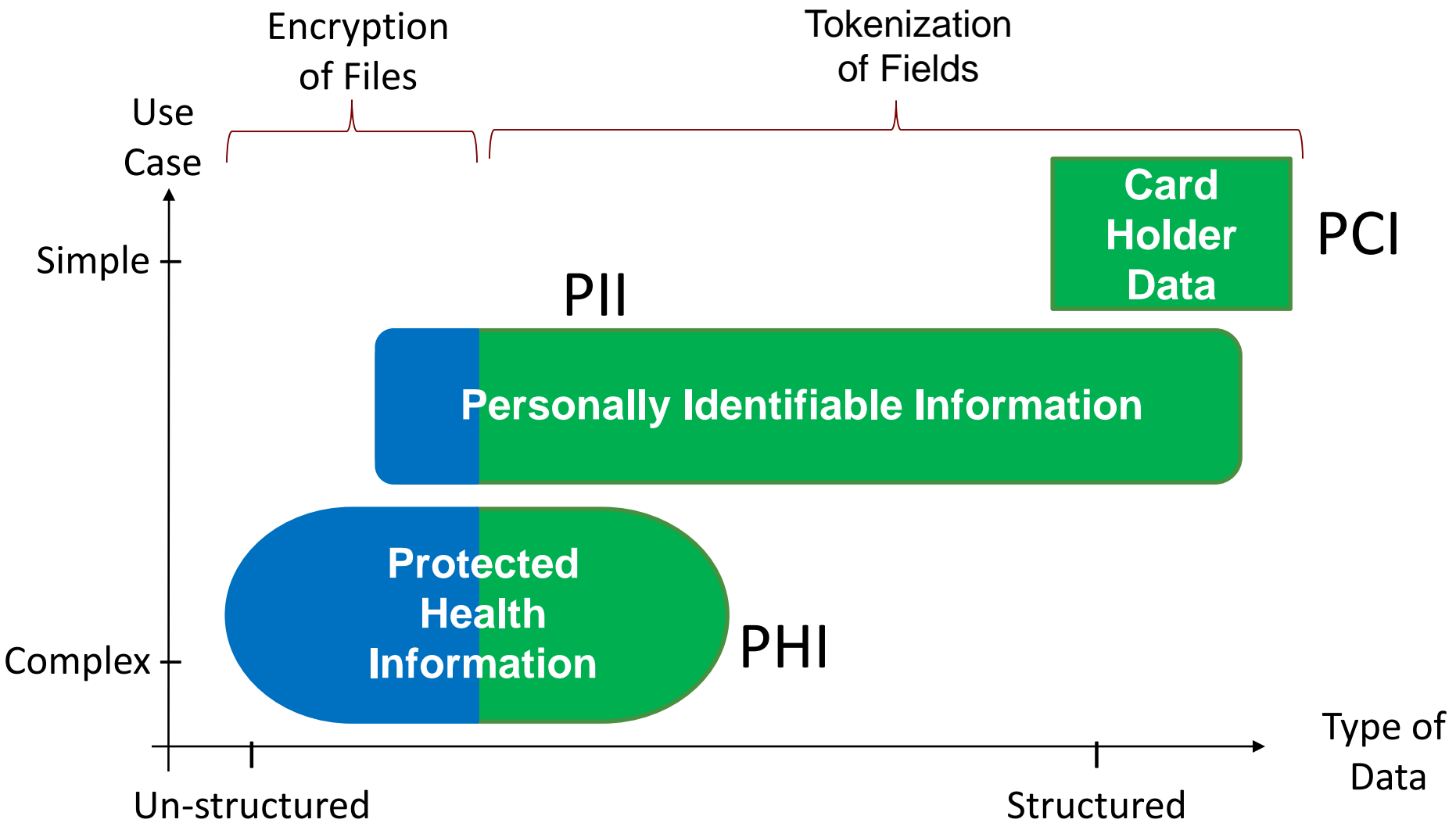
Vaultless

Property	Dynamic	Pre-generated	Vaultless
Footprint	Large, Expanding	Large, Static	Small, Static
Replication	Complex replication required	No replication required	No replication required
Collisions	Prone to collisions	No collisions	No collisions
Latency / Performance	Will impact performance and scalability	Will impact performance and scalability Faster than the traditional dynamic approach	Little or no latency Fastest tokenization in the industry
Tokenizing many data categories	Potentially impossible	Potentially impossible	Can tokenize many data categories with minimal or no impact on footprint or performance




Threat Landscape



How Should I Secure Different Data?



Examples: De-Identified Sensitive Data

Field	Real Data	Tokenized / Pseudonymized
Name	Joe Smith	csu wusoj
Address	100 Main Street, Pleasantville, CA	476 srta coetse, cysieondusbak, CA
Date of Birth	12/25/1966	01/02/1966
Telephone	760-278-3389	760-389-2289
E-Mail Address	joe.smith@surferdude.org	eo.e.nwuer@beusorpdqo.org
SSN	076-39-2778	076-28-3390
CC Number	3678 2289 3907 3378	3846 2290 3371 3378
Business URL	www.surferdude.com	www.sheyinctao.com
Fingerprint		Encrypted
Photo		Encrypted
X-Ray		Encrypted
Healthcare / Financial Services	Dr. visits, prescriptions, hospital stays and discharges, clinical, billing, etc. Financial Services Consumer Products and activities	Protection methods can be equally applied to the actual data, but not needed with de-identification

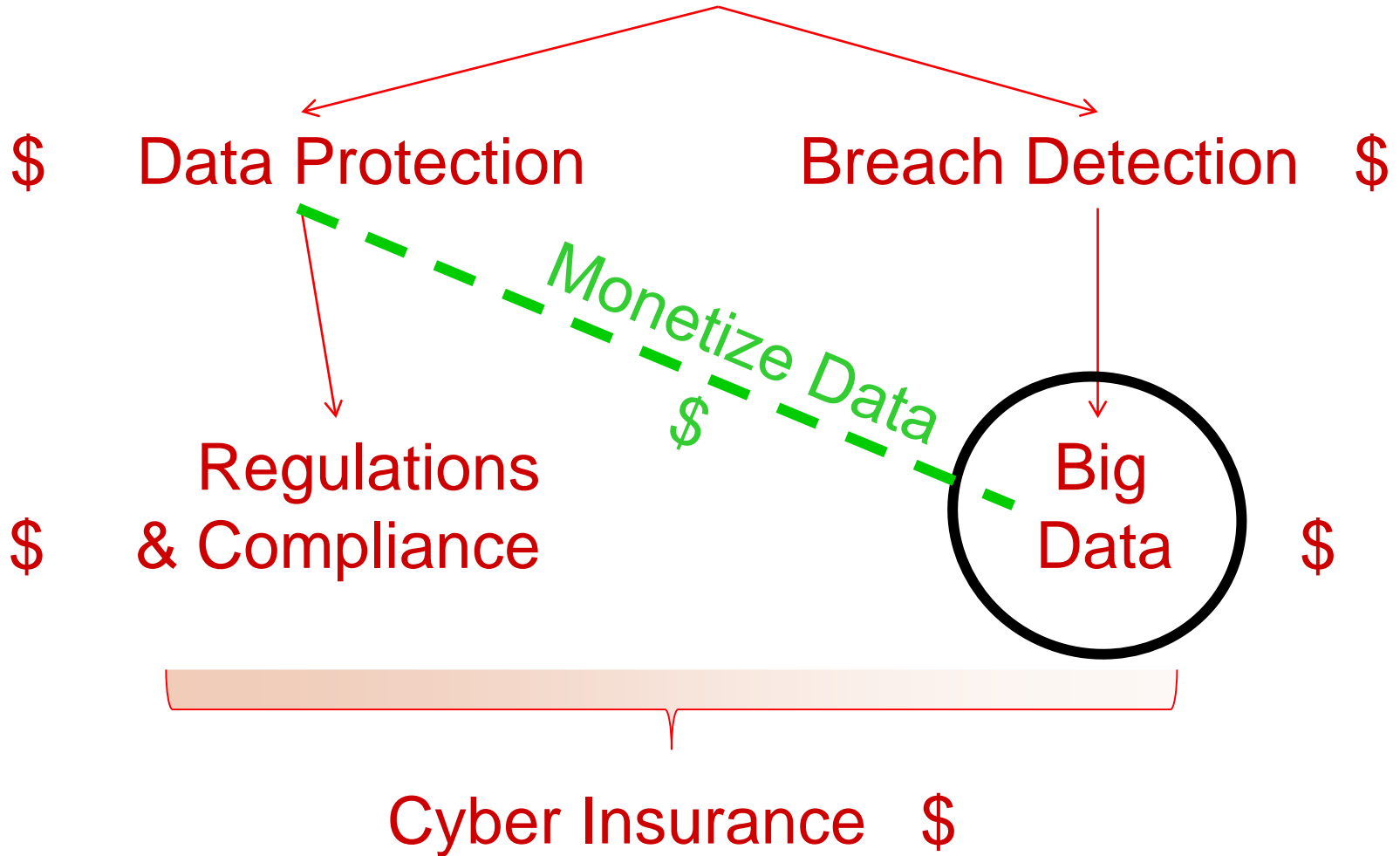
Health Information Portability and Accountability Act (HIPAA)

- USA law, originally passed in 1996
- Defines “Protected Health Information” (PHI)
- Updated by the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009
- Most recently, the Omnibus final rule came into effect September 2013
- Now requires both organizations that handle PHI and their business partners to protect sensitive information

US Health Information Portability and Accountability Act – HIPAA

1. Names
2. All geographical subdivisions smaller than a State
3. All elements of dates (except year) related to individual
4. Phone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social Security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger prints
17. Full face photographic images
18. Any other unique identifying number

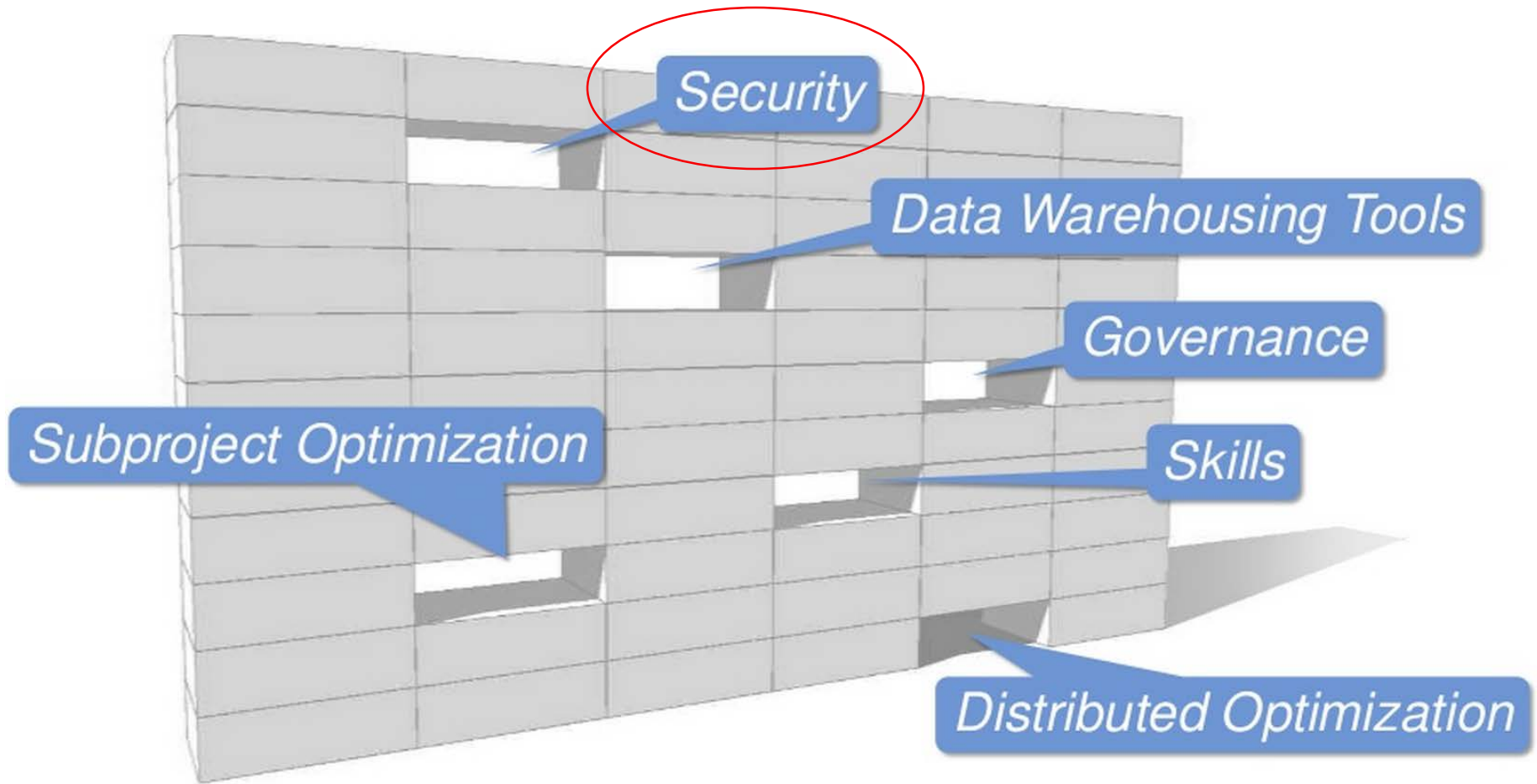
Threat Landscape



THE CHANGING TECHNOLOGY LANDSCAPE

What effect, if any, does the rise of “Big Data” have on breaches?

Holes in Big Data...



Source: Gartner

Many Ways to Hack Big Data



Hackers
& APT

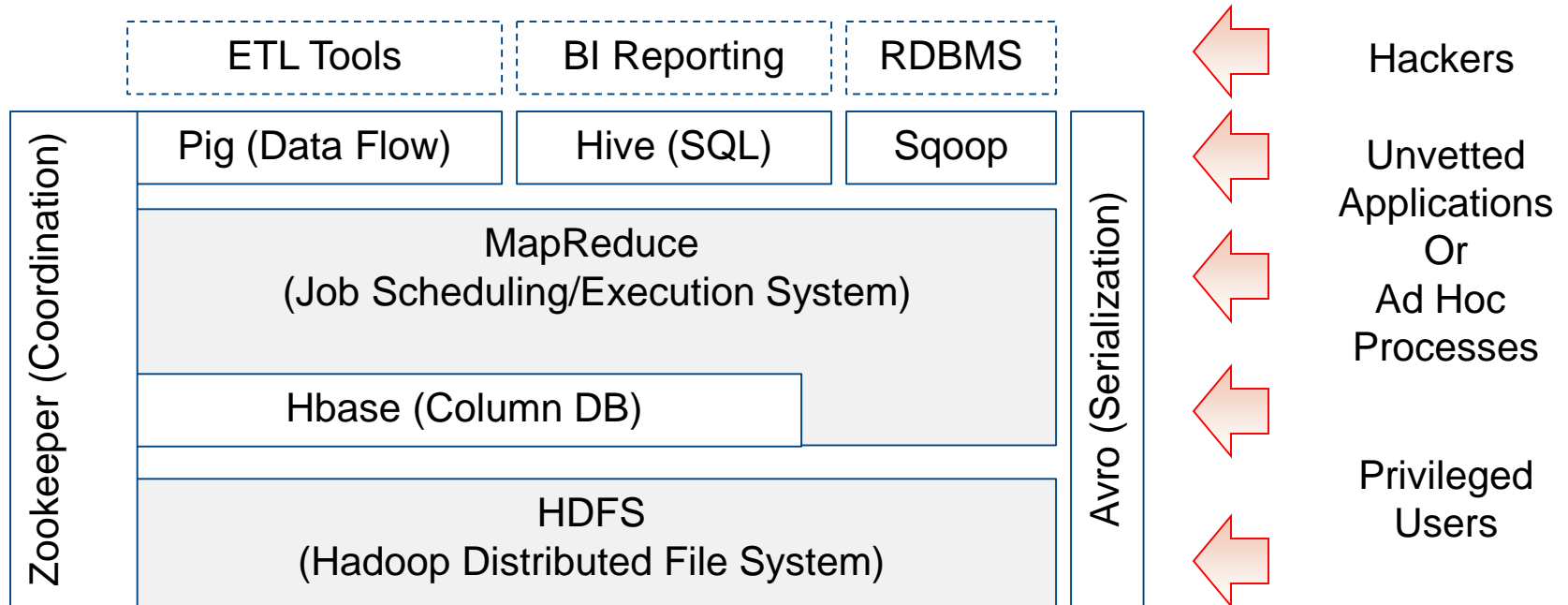


Unvetted
Applications
Or
Ad Hoc
Processes



Rogue
Privileged
Users

Many Ways to Hack Big Data



Source: <http://nosql.mypopescu.com/post/1473423255/apache-hadoop-and-hbase>

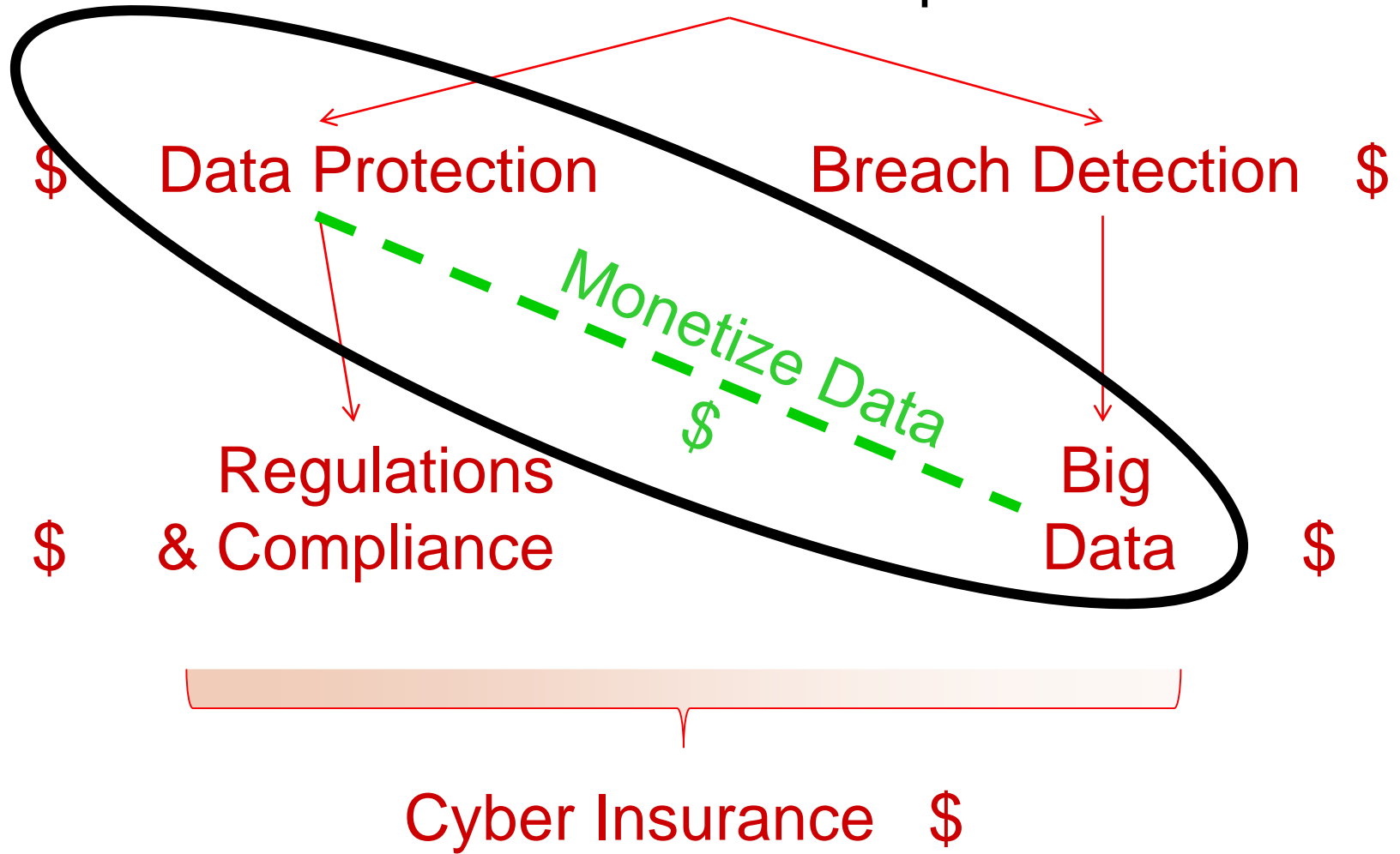
Big Data Vulnerabilities and Concerns

- Big Data (Hadoop) was designed for data access, not security
- Security in a read-only environment introduces new challenges
- Massive scalability and performance requirements
- Sensitive data regulations create a barrier to usability, as data cannot be stored or transferred in the clear
- Transparency and data insight are required for ROI on Big Data

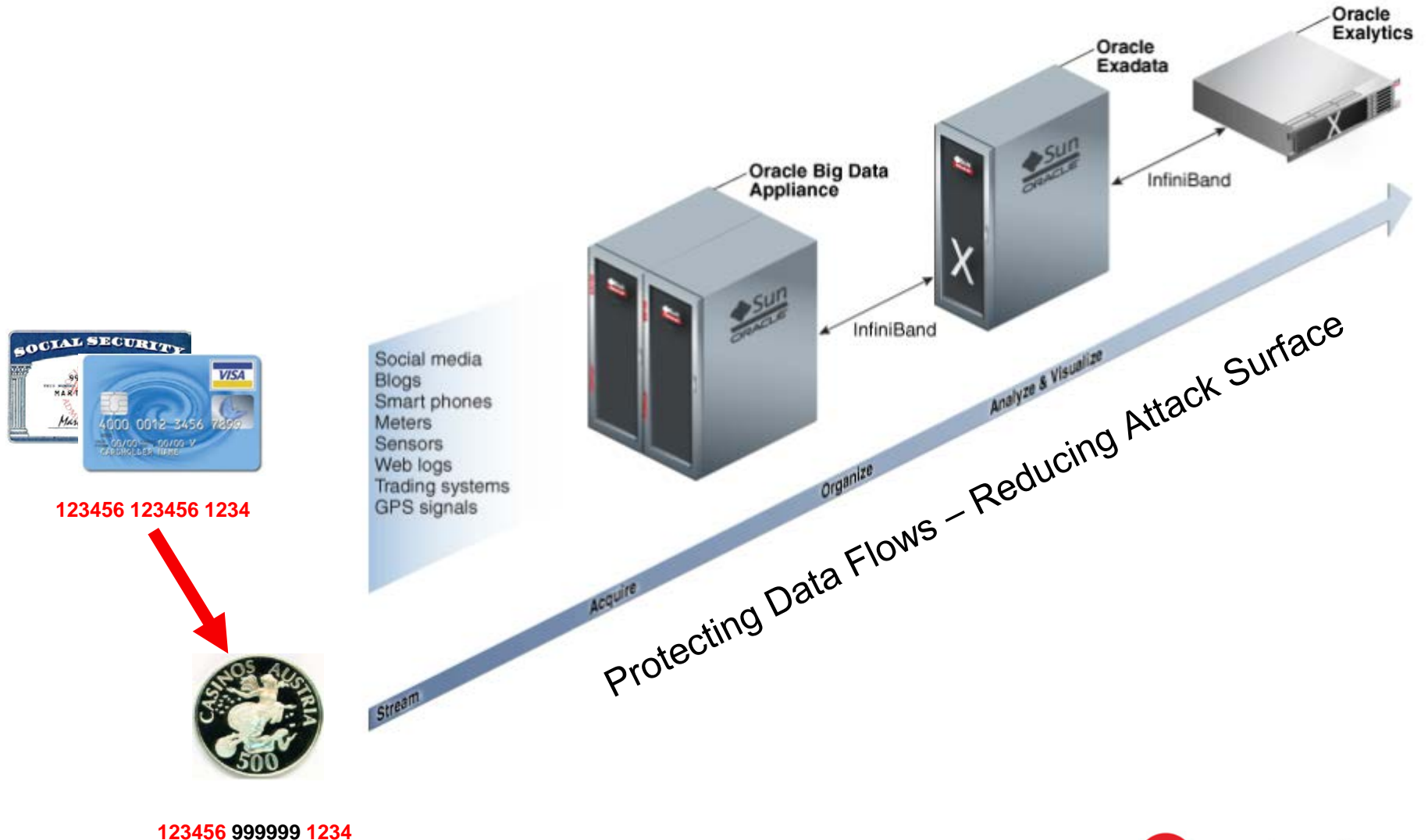
BIG DATA

*Protecting the data flow
&
Catching attackers*

Threat Landscape



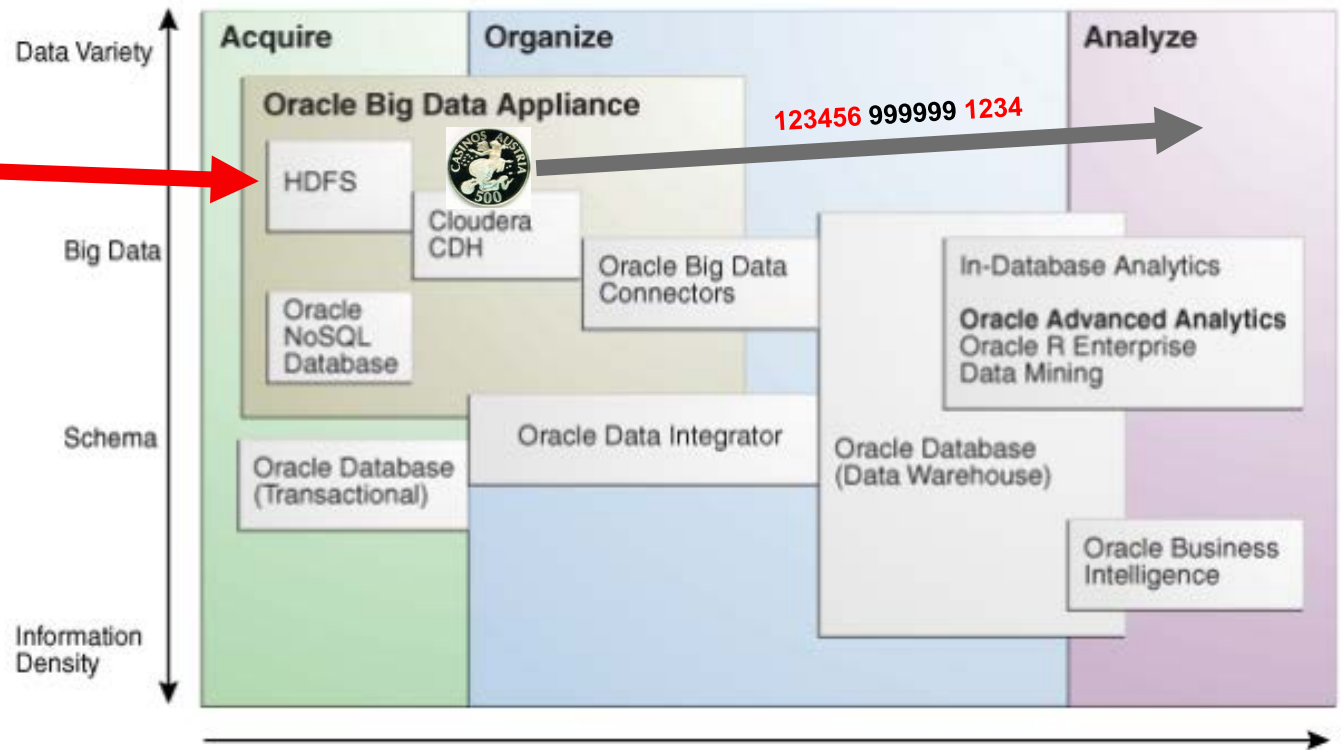
Oracle's Big Data Platform



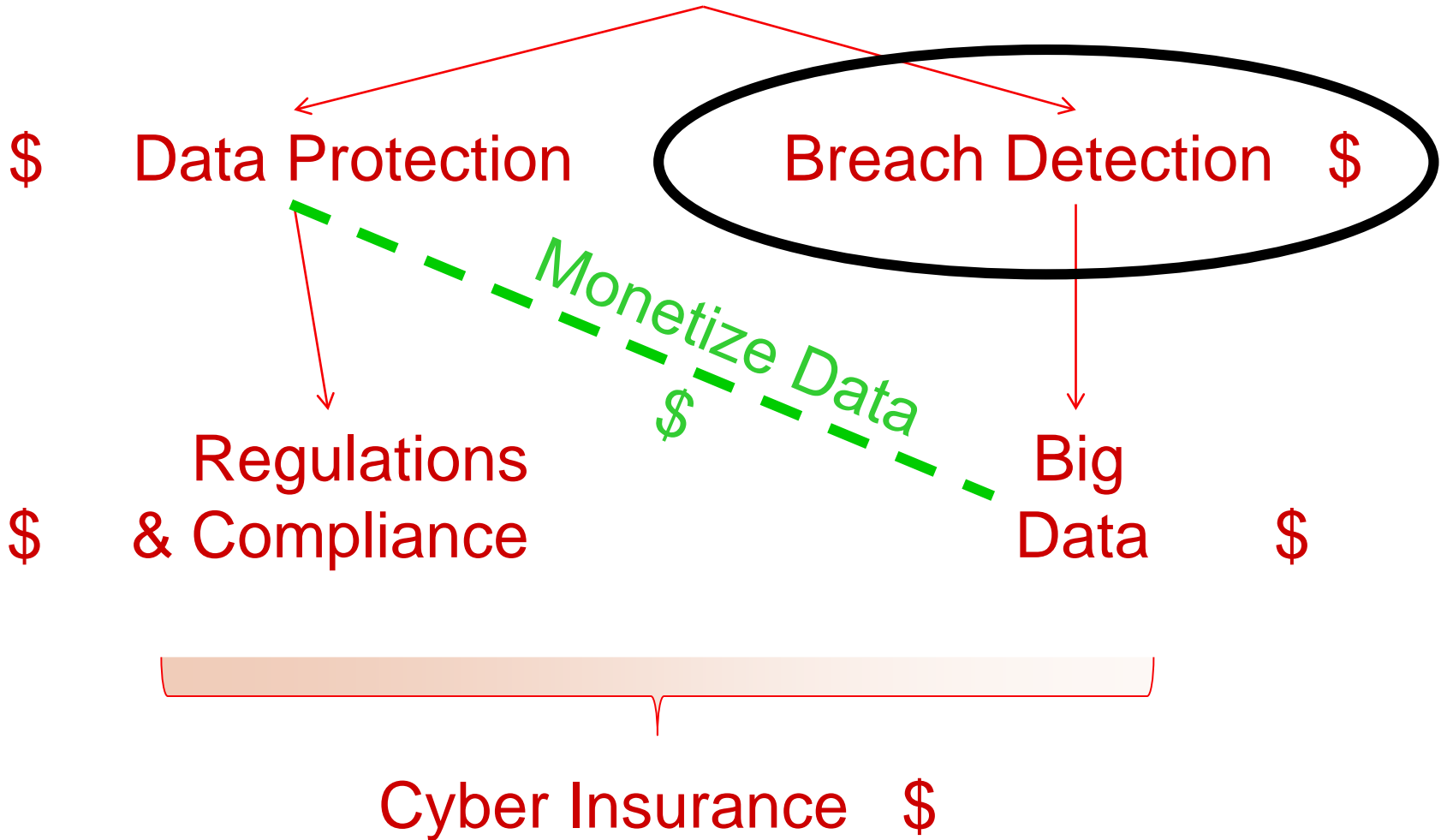
Tokenization Reducing Attack Surface



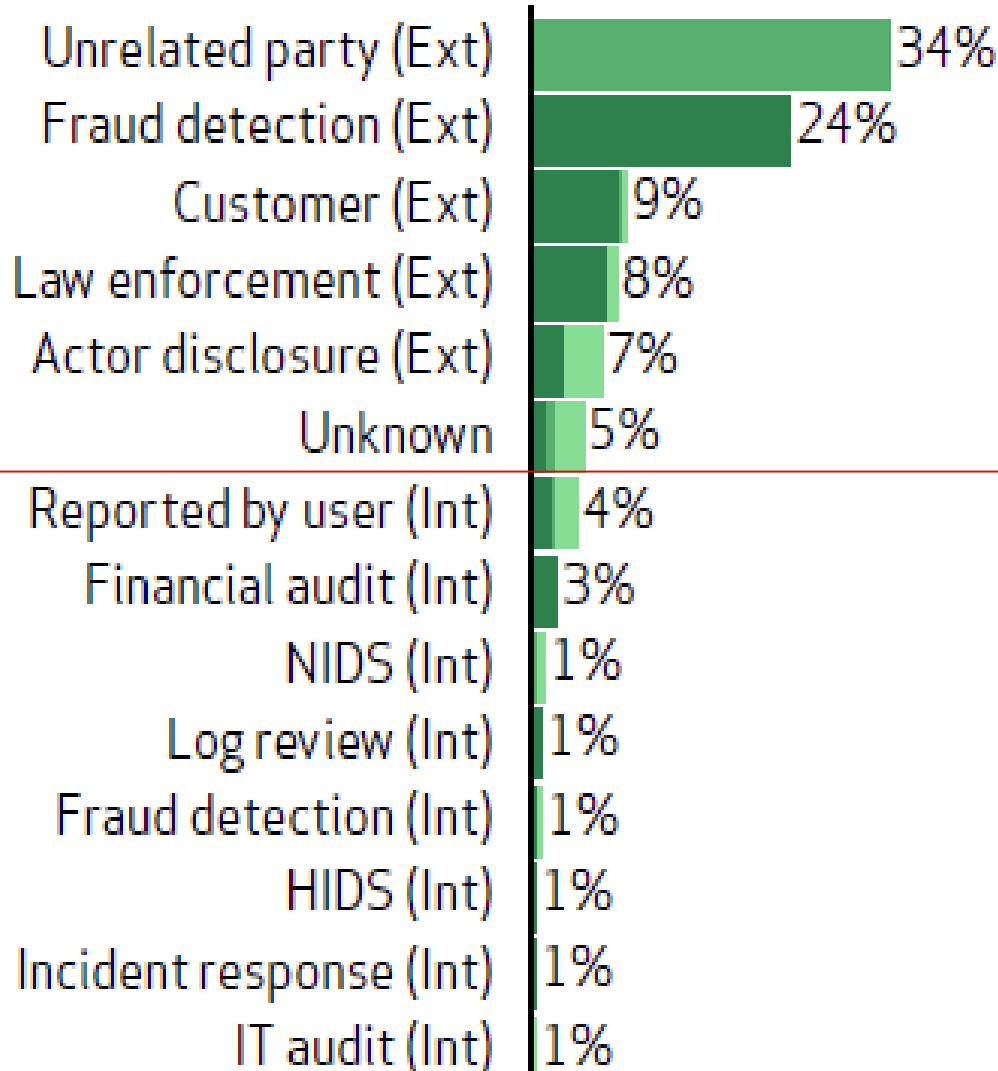
Tokenization on Each Node



Threat Landscape



Current Breach Discovery Methods

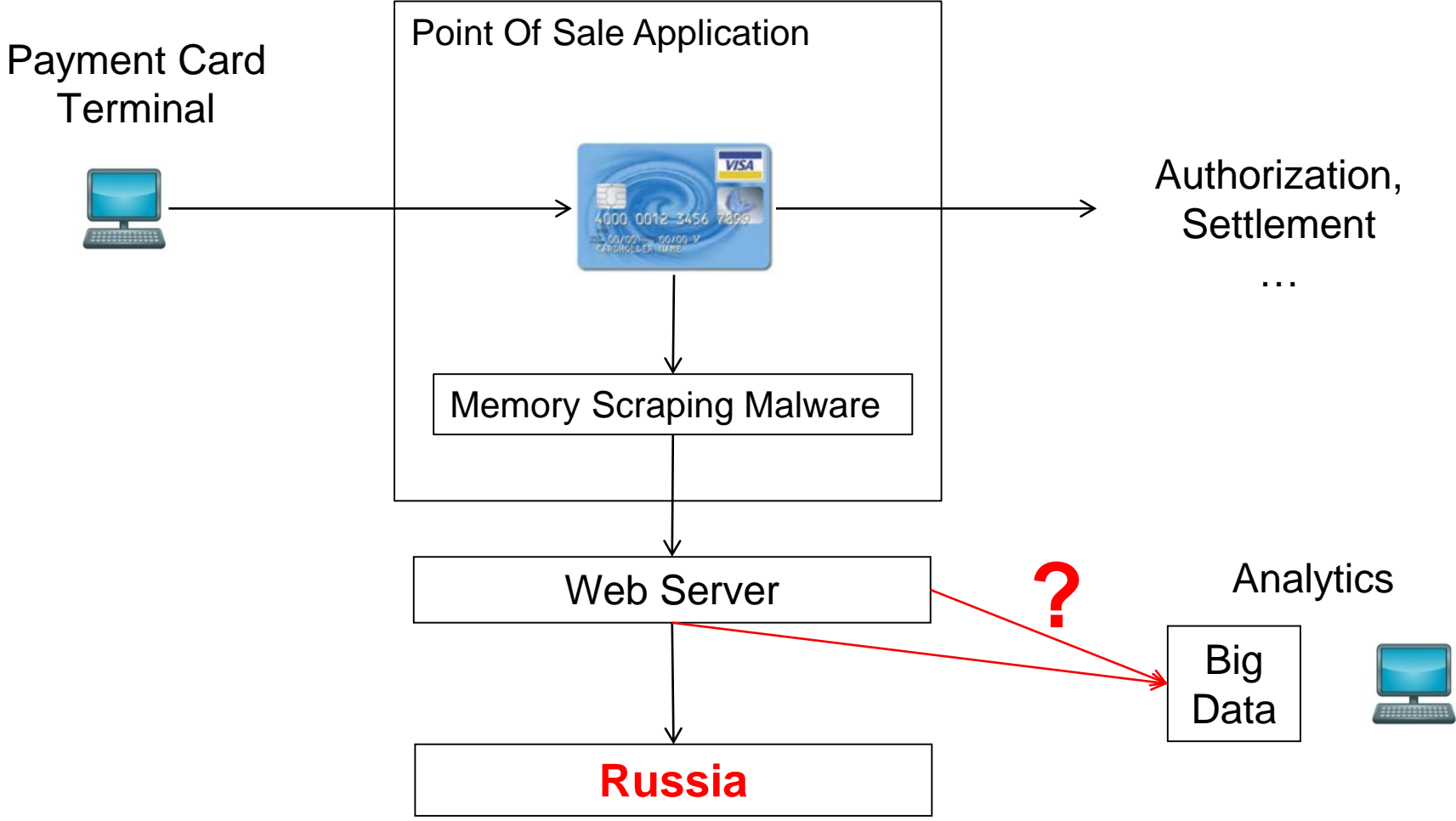


■ Financial ■ Espionage ■ Other

Verizon 2013 Data-breach-investigations-report & 451 Research



Use Big Data to Analyze Abnormal Usage Pattern

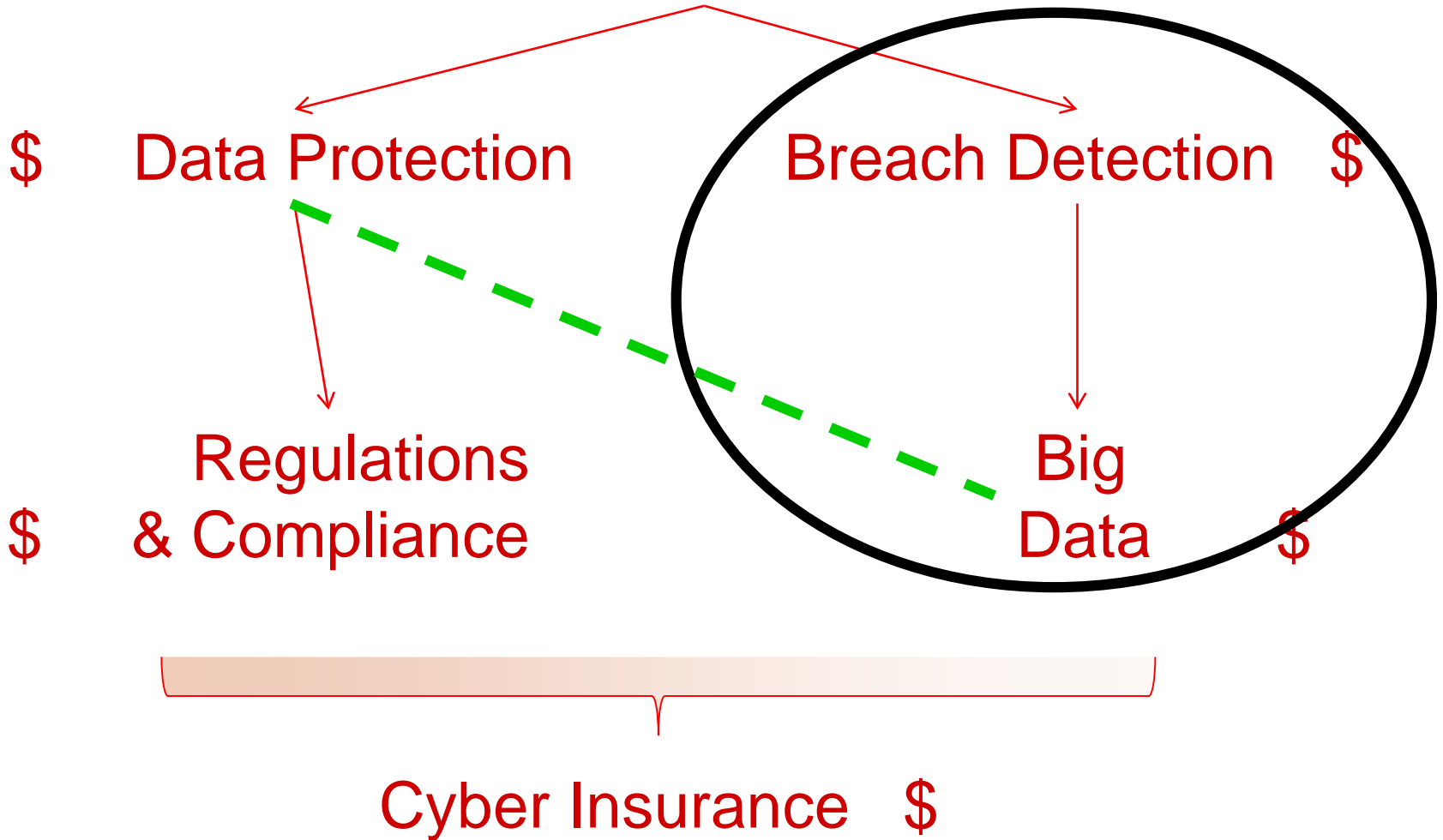


CISOs say SIEM Not Good for Security Analytics

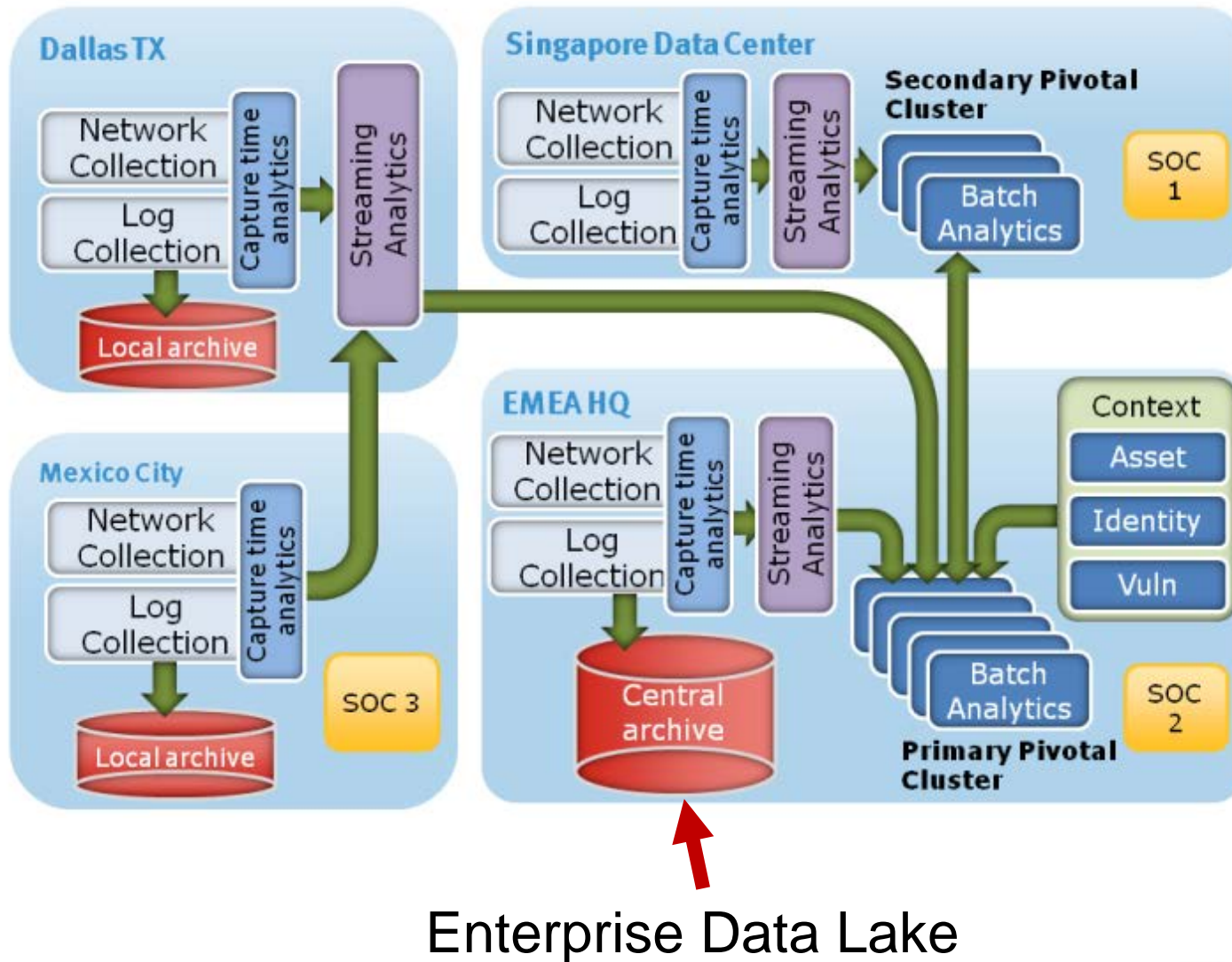
- You must assume the systems will be breached.
- Once breached, how do you know you've been compromised?
- You have to baseline and understand what 'goodness' looks like and look for deviations from goodness
- McAfee and Symantec can't tell you what normal looks like in your own systems.
- Only monitoring anomalies can do that
- Monitoring could be focused on a variety of network and end-user activities, including network flow data, file activity and even going all the way down to the packets

Source: 2014 RSA Conference, moderator Neil MacDonald, vice president at Gartner

Threat Landscape



Open Security Analytics Framework & Big Data



Conclusions

○ **What happened at Target?**

- Modern customized malware can be very hard to detect
- They were compliant, but not secure

○ **Changing threat landscape & challenges to secure data:**

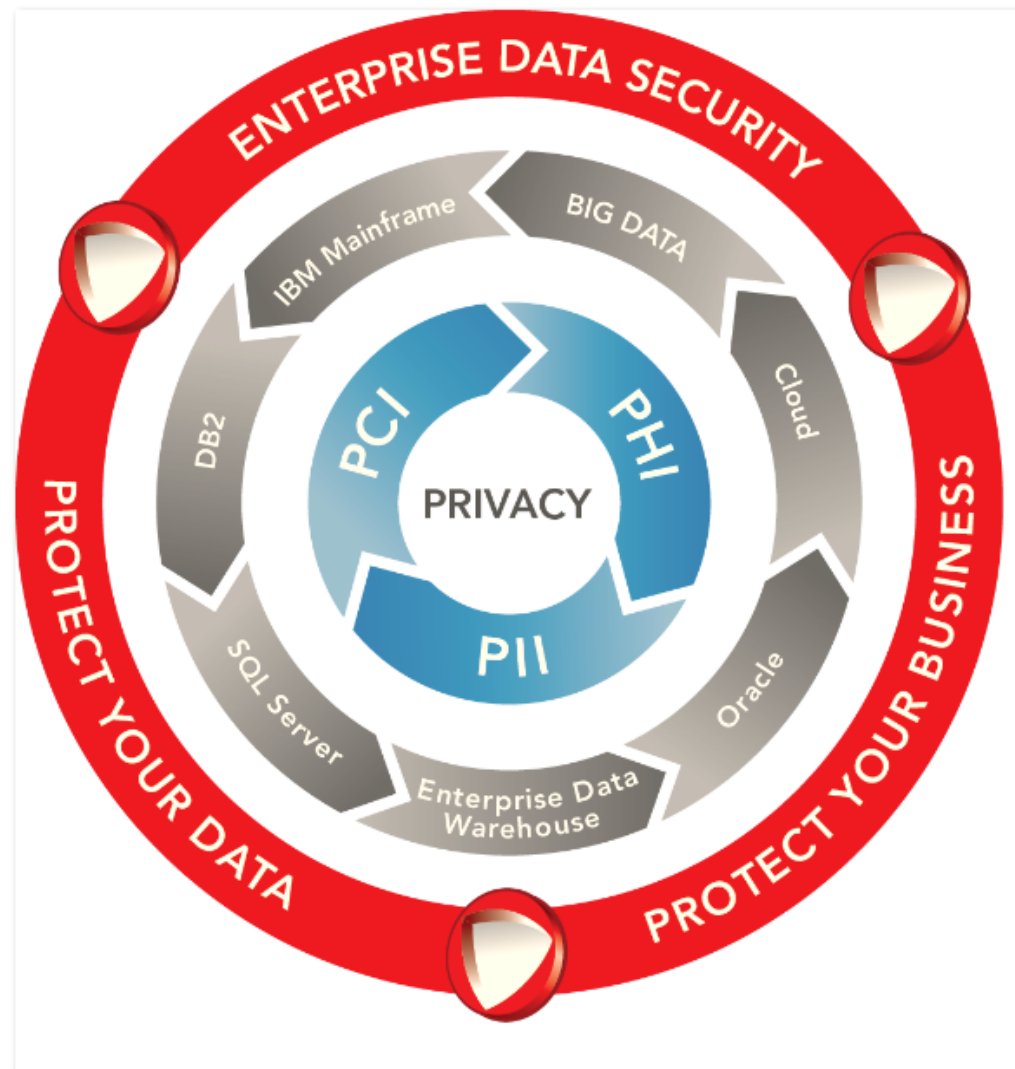
- Attackers are looking for not just payment data – a more serious problem.
- IDS systems are lacking context needed to catch data theft
- SIEM detection is too slow in handling large amounts of events.

○ **How can we prevent what happened to Target and the next attack against our sensitive data?**

- Assume that we are under attack - proactive protection of the data itself
- We need to analyze event information and context to catch modern attackers
- The Oracle Big Data Appliance can provide the foundation for solving this problem

Protegrity Summary

- Proven enterprise data security software and innovation leader
 - Sole focus on the protection of data
 - Patented Technology, Continuing to Drive Innovation
- Cross-industry applicability
 - Retail, Hospitality, Travel and Transportation
 - Financial Services, Insurance, Banking
 - Healthcare
 - Telecommunications, Media and Entertainment
 - Manufacturing and Government





Thank you!

Questions?

Please contact us for more information

<http://www.protegrity.com/news-resources/collateral/>

Ulf.Mattsson AT protegrity.com



protecting your **data.**
protecting your **business.**