

RSAConference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: PDAC-F01

Place Your Bets on Tokenization to Improve Cybersecurity



Connect **to**
Protect

John Kindervag

Vice President & Principal Analyst
Forrester Research, Inc.
@Kindervag



#RSAC



What is Tokenization?



PAN

4672564304618386

Tokenized

467256GH3LKK8386

FPE or token

9810143588110281



Data Security was driven by PCI



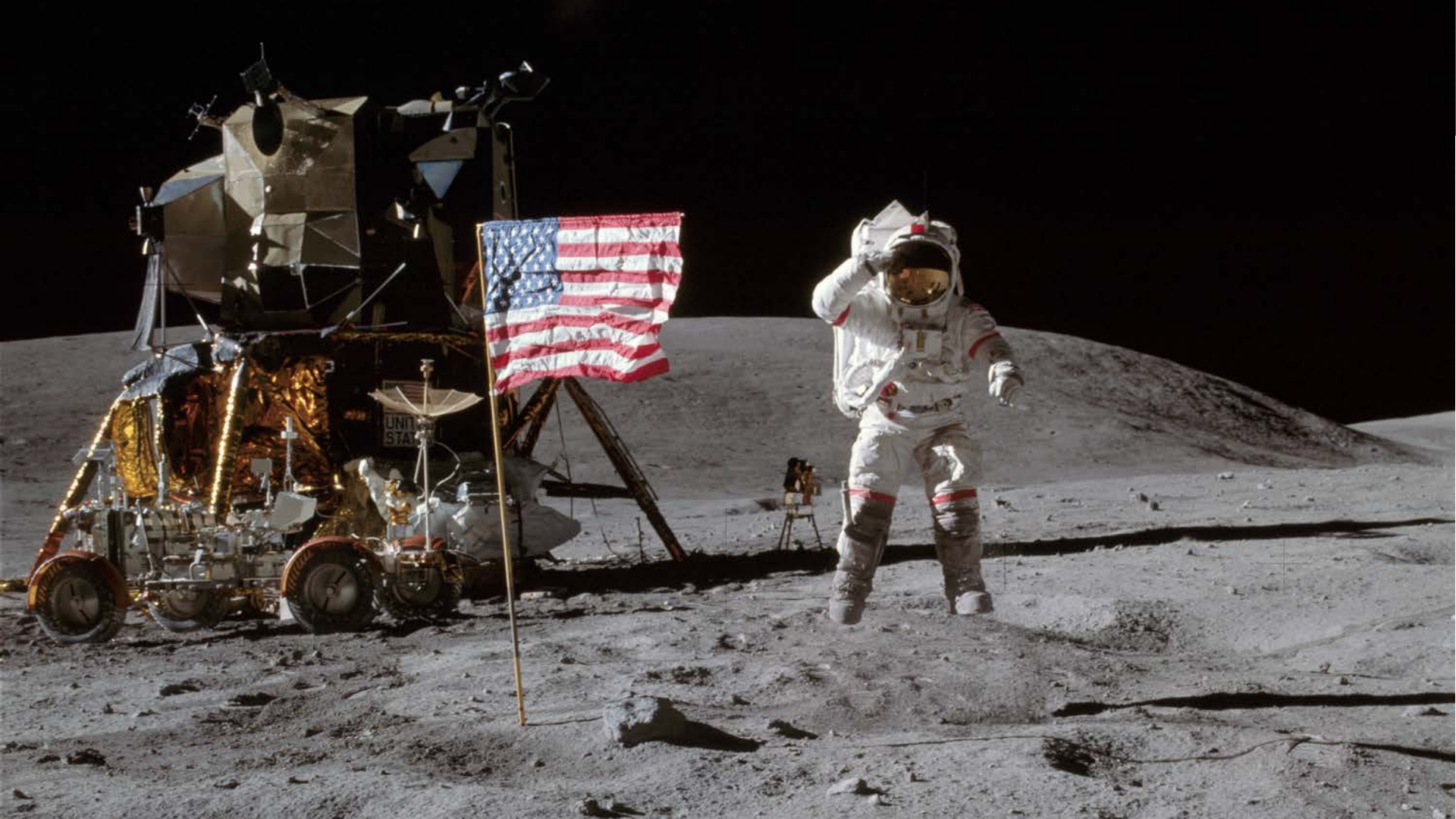
#RSAC

Why PCI DSS 3.0?

To stay competitive in terms of security and compliance, organizations need a structured, predictable, and continuous approach to solving ongoing challenges that's easy enough to do every day. By raising security standards and making PCI DSS compliance the status quo, organizations can monitor the effectiveness of their security controls and maintain their PCI DSS compliant environment.



PCI DSS 3.0 helps organizations focus on security, not compliance, by making payment security **business-as-usual**. How?





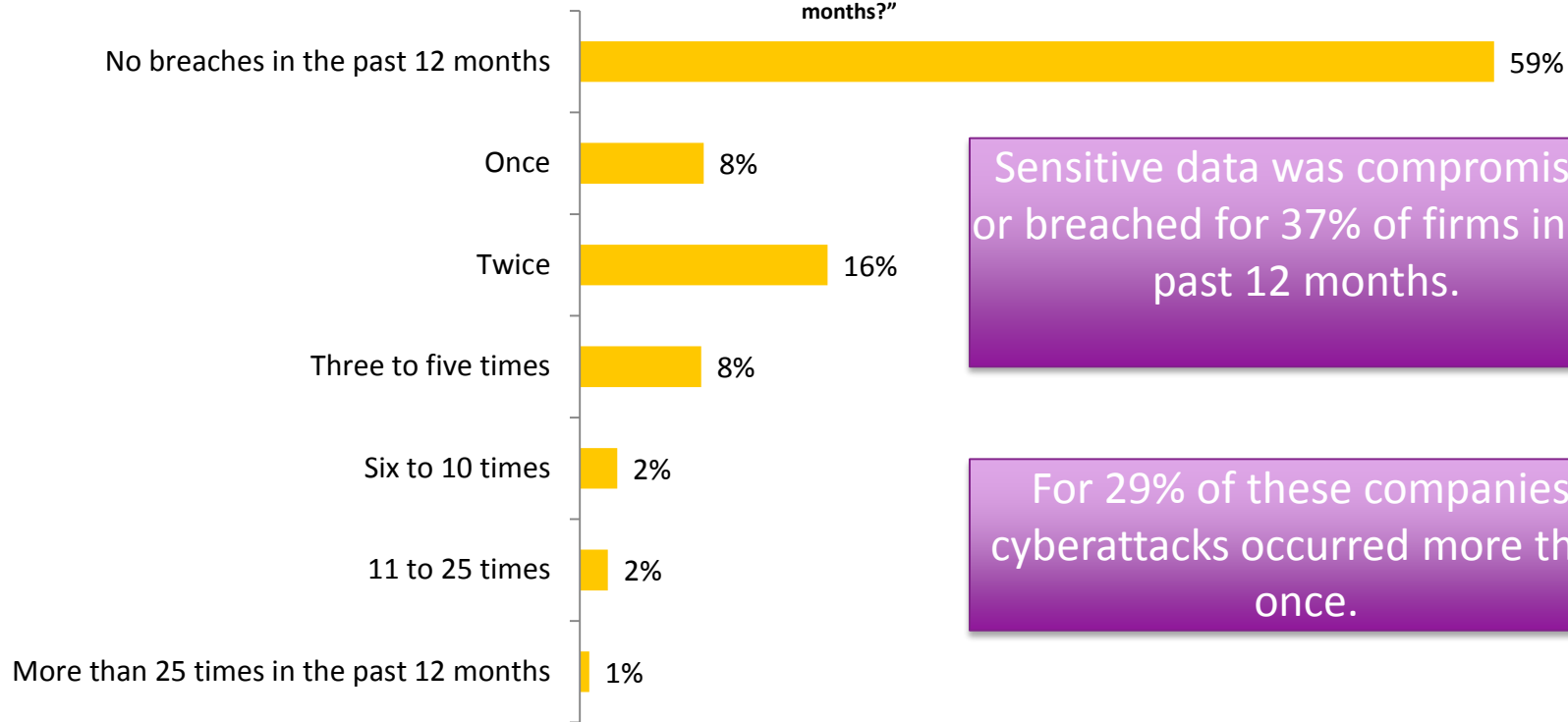


Breaches Happen



#RSAC

“How many times do you estimate that your firm’s sensitive data was potentially compromised or breached in the past 12 months?”



Sensitive data was compromised or breached for 37% of firms in the past 12 months.

For 29% of these companies, cyberattacks occurred more than once.

Base: 166 director+ security decision-makers in the US in firms with more than 100 employees
Source: Forrester's Global Business Technographics Security Survey, 2015 (Note: Not showing "Don't know")



File View Favorites Tools Commands Window Help

Log: ***** 313 ms

EFNet cRiND
Channels: 9
#ccpower
#fw
#Gangsta
#had2600
#LinuxShell
#sharktech
#shelt
#underground
#unixshells
Queries: 0

ircuNknDwn.ws cRiND
Channels: 1
#unkrDwn
Queries: 0

DALnet cRiND
Channels: 1
#ccpower
Queries: 0

PCIRC cRiND
Channels: 1
#ccpower
Queries: 0

HackCrew cRiND
Channels: 1
#ccpower
Queries: 0

DCCs: 0
Gets: 0
Sends: 0
Chats: 0
FTPd: Offline
Clients: 0/2

```

1:44p (%SUFU) Selling cvv worldwide & Dumps T18T2 & Shell C99 Only Worldwide socks payment LR / W
1:44p (AdvBot) Random Message: Warning! We Do Not Take Responsibility For Anything In This Server! You Are The Only Responsible Here!
1:44p (AdvBot) Random Message: Don't Deal With Unregistered Hackers! Need Help? Ask An Oper
1:44p (AdvBot) Random Message: Look! We have got a new copy of 2013-2014's New Hack
1:44p (AdvBot) [Napster] link a good web hosting, domain names, game servers, teampeak, proxy, vpn, can make you make cheap proxy
1:44p + AbuJee Selling ( Worldwide Cvv,Worldwide Fullz, UK,Usa Logins Worldwide Dumps, UK,Usa Paypal, Ebay Accounts, Worldwide Fresh
socks UK Dab Look Up, Usa Dob,Ssn,Mmn,Etc LookUp Payment Method LR<<<WMZ<<<>WU<<<>Only
1:44p (AdvBot) [Napster] Buying Carded Counter Strike 1.6 Servers!! Also Buying World Of Warcraft CD Keys!! Msg Napster
1:44p + AbuJee Selling ( Worldwide Cvv,Worldwide Fullz, UK,Usa Logins Worldwide Dumps, UK,Usa Paypal, Ebay Accounts, Worldwide Fresh
socks UK Dab Look Up, Usa Dob,Ssn,Mmn,Etc LookUp Payment Method LR<<<WMZ<<<>WU<<<>Only
1:44p (host) iq 410532559
1:44p (%SUFU) Selling cvv worldwide & Dumps T18T2 & Shell C99 Only Worldwide socks payment LR / W
1:44p (host) selling fullz cc
1:44p (host) selling login us,uk
1:44p (host) selling fresh vergin
1:44p (host)
1:44p (host)
1:44p (host)
1:44p (host)
1:44p (host)
1:44p (host)
1:44p (host)
1:44p (AdvBot) Selling SHIP Send Inbox, PHP Mailer Send All Inbox, (hacksoft/try/freemall/cpanel), Fresh Unpaired UK/US Mail List from Shopmail CB
1:44p (%SUFU) SHIP (99 $) Hackd Root, UK/US Remote Desktop (Vista/XP), Fresh UK/US Full CC, Fresh UK/US CCV, Payment Liberty Reserve
1:44p (host) selling fresh vergin worldwide cvv
1:44p (host) selling fresh vergin worldwide cvv
1:44p (%SUFU) TheWhiteCo I am seller CVV, UK Banks, Fresh UK/USA Leads, Email Access Selected, I cash out WU UK/India in anytime
1:44p (Valladeum) Selling SHIP Send Inbox, PHP Mailer Send All Inbox, (hacksoft/try/freemall/cpanel), Fresh Unpaired UK/US Mail List from Shopmail CB
1:44p (%SUFU) SHIP (99 $) Hackd Root, UK/US Remote Desktop (Vista/XP), Fresh UK/US Full CC, Fresh UK/US CCV, Payment Liberty Reserve
1:44p (Valladeum) Selling SHIP Send Inbox, PHP Mailer Send All Inbox, (hacksoft/try/freemall/cpanel), Fresh Unpaired UK/US Mail List from Shopmail CB
1:44p (%SUFU) SHIP (99 $) Hackd Root, UK/US Remote Desktop (Vista/XP), Fresh UK/US Full CC, Fresh UK/US CCV, Payment Liberty Reserve
1:44p (host) GOOD OFFER! SELLING hacked RDP GUARANTEED 24HOURS UP TIME ONLY 10$
1:44p (AdvBot) mainower is catching bank of America Logins, Western Europe Logins,LOYDS Logins,Natwest Logins,Jaffas Logins, Interested New
mainower is catching bank of America Logins, Western Europe Logins,LOYDS Logins,Natwest Logins,Jaffas Logins, Interested New
1:44p (JunatedStates) I need RDP UK US Germany To buy NOW VIA LR WMZ wana buy 9
1:44p (JunatedStates) I need RDP UK US Germany To buy NOW VIA LR WMZ wana buy 9
1:44p (JunatedStates) I need RDP UK US Germany To buy NOW VIA LR WMZ wana buy 9
1:44p (JunatedStates) I need RDP UK US Germany To buy NOW VIA LR WMZ wana buy 9
1:44p (JunatedStates) I need RDP UK US Germany To buy NOW VIA LR WMZ wana buy 9
1:44p (JunatedStates) I need RDP UK US Germany To buy NOW VIA LR WMZ wana buy 9
1:44p + AbuJee Selling ( Worldwide Cvv,Worldwide Fullz, UK,Usa Logins Worldwide Dumps, UK,Usa Paypal, Ebay Accounts, Worldwide Fresh
socks UK Dab Look Up, Usa Dob,Ssn,Mmn,Etc LookUp Payment Method LR<<<WMZ<<<>WU<<<>Only
1:44p + AbuJee Selling ( Worldwide Cvv,Worldwide Fullz, UK,Usa Logins Worldwide Dumps, UK,Usa Paypal, Ebay Accounts, Worldwide Fresh
socks UK Dab Look Up, Usa Dob,Ssn,Mmn,Etc LookUp Payment Method LR<<<WMZ<<<>WU<<<>Only
1:44p (host) selling fresh vergin worldwide cvv
1:44p (host) selling fresh vergin worldwide cvv

```

Selling (Worldwide Cvv, Worldwide Fullz,
UK, Usa Logins Worldwide Dumps, UK,
Usa Paypal, Ebay Accounts...)

There are only Two Types of Data



#RSAC



Data that someone **wants** to steal



Everything else

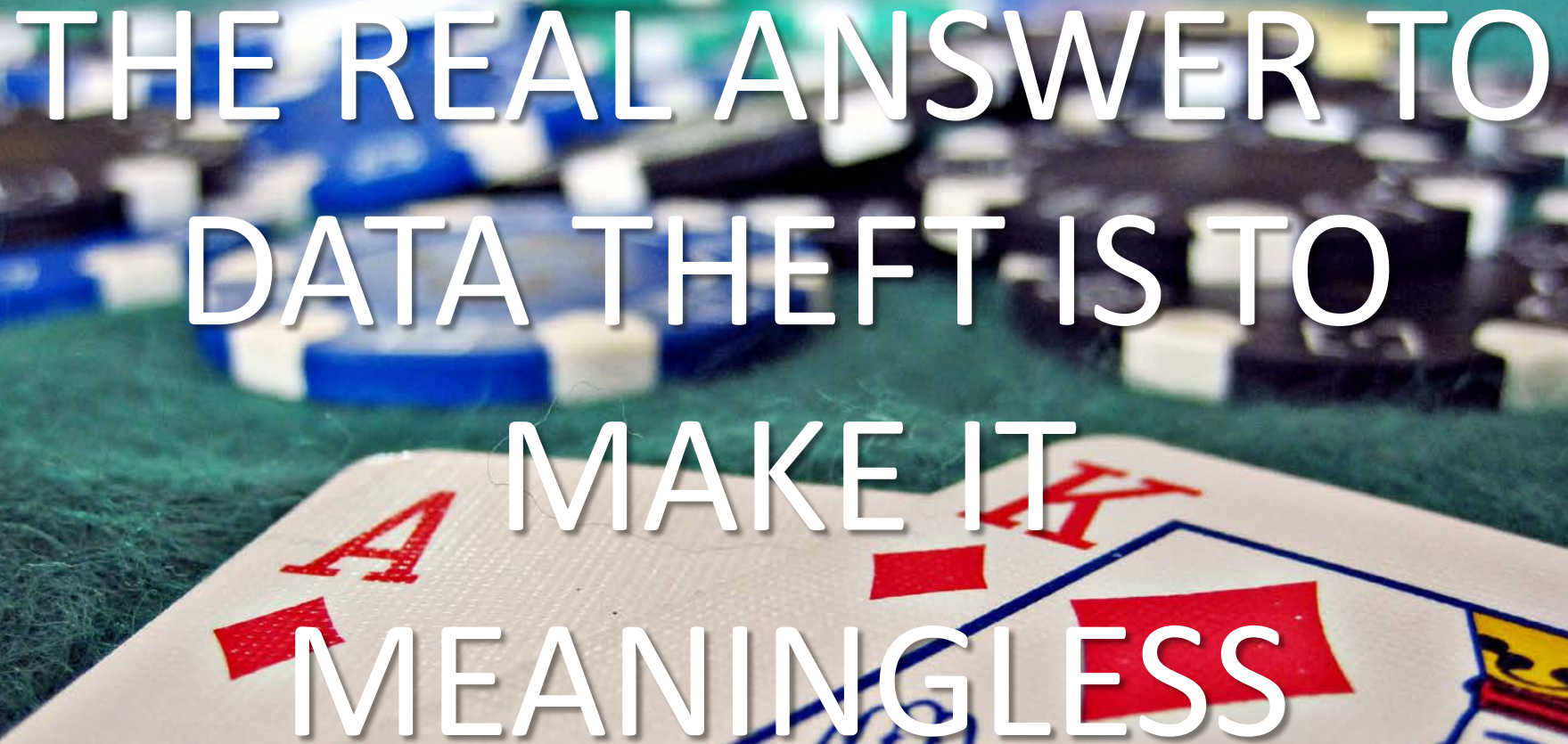
Cybercriminals Steal Toxic Data



■ Remember the Four P's:

- PCI
- PHI
- PII
- IP

$$3P + IP = TD$$

The image shows a close-up, slightly blurred view of a casino table. In the foreground, a playing card, the Ace of Spades, is visible with its red 'A' and spade symbol. To the right, another card, the King of Spades, is partially visible. The background is filled with numerous blue and white chips scattered across a green felt surface. Overlaid on this scene is the text 'THE REAL ANSWER TO DATA THEFT IS TO MAKE IT MEANINGLESS' in a large, white, sans-serif font.

THE REAL ANSWER TO
DATA THEFT IS TO
MAKE IT
MEANINGLESS

Encryption Covers A Multitude Of Sins



#RSAC

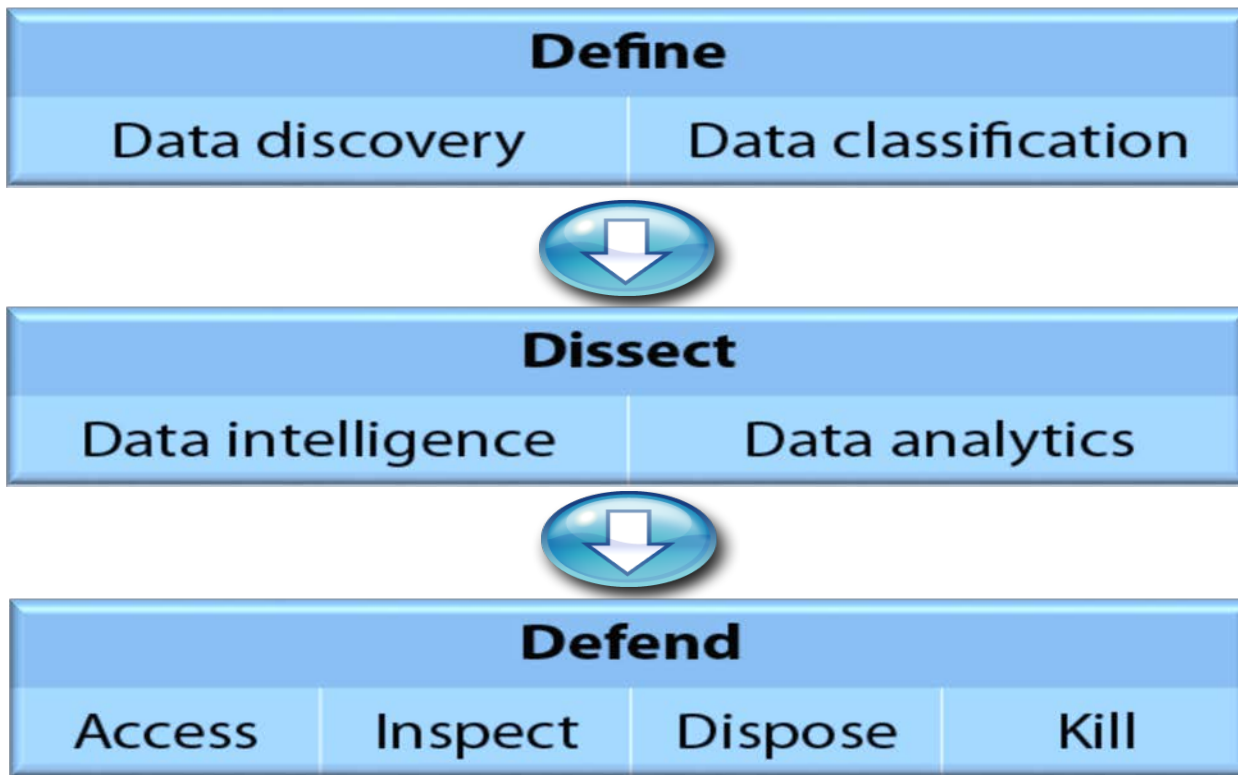
California SB 1386

“This bill, operative July 1, 2003, would require a state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information, as defined, to disclose in specified ways, any breach of the security of the data, as defined, to any resident of California whose **unencrypted personal information** was, or is reasonably believed to have been, acquired by an unauthorized person.”

Big data security and control framework



#RSAC





- Encryption
- Masking
- Tokenization

Data Abstraction

Source: January 26, 2012, "The Future Of Data Security And Privacy: Controlling Big Data" Forrester report

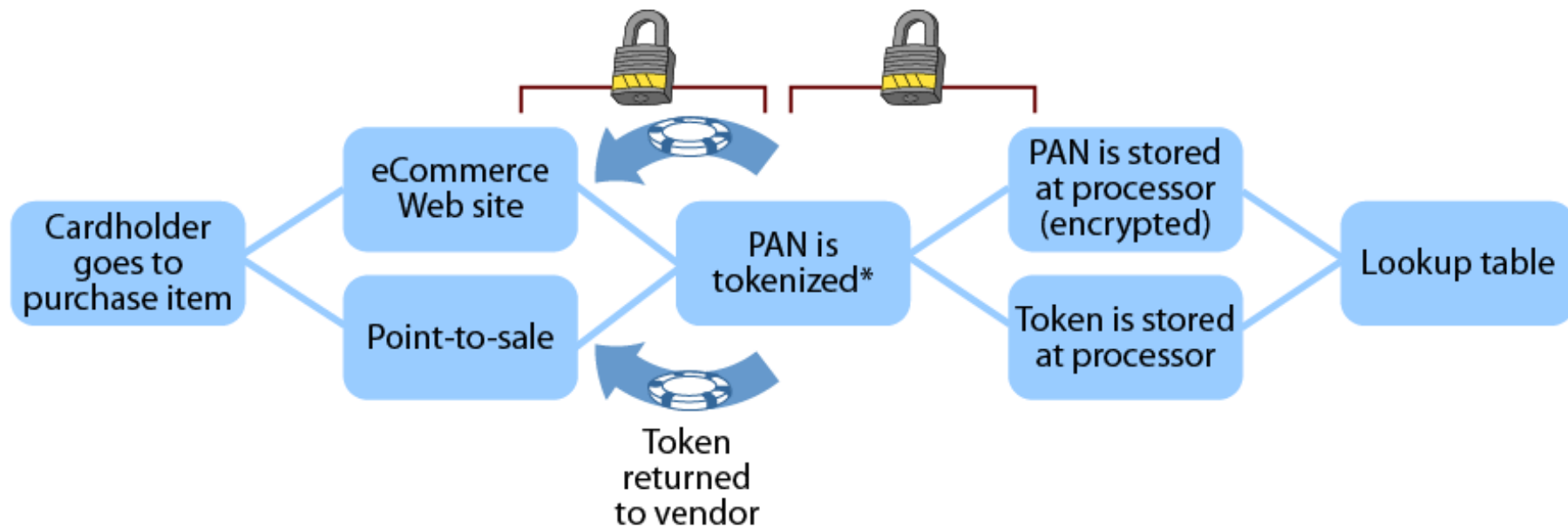
Tokenization vs. Encryption

PAN	4672564304618386	16
Tokenized	467256GH3LKK8386	16
In binary	10000100110011010110000100111100100010010001110010010	53
Padded for AES	000 0000000000010000100110011010110000100111100100010010001110010010	128
AES encrypted	0101011001000000111010011110010110011100101111011001110110110000 1000111101001010000011110010100101101011111010011111001011110100	128
FPE or token	9810143588110281	16

Tokenization High-Level Flow



#RSAC



*Token is returned to merchant payment system and stored by processor

April 2010 "Demystifying Tokenization And Transaction Encryption, Part 1: Get Ready To Place Some Bets"

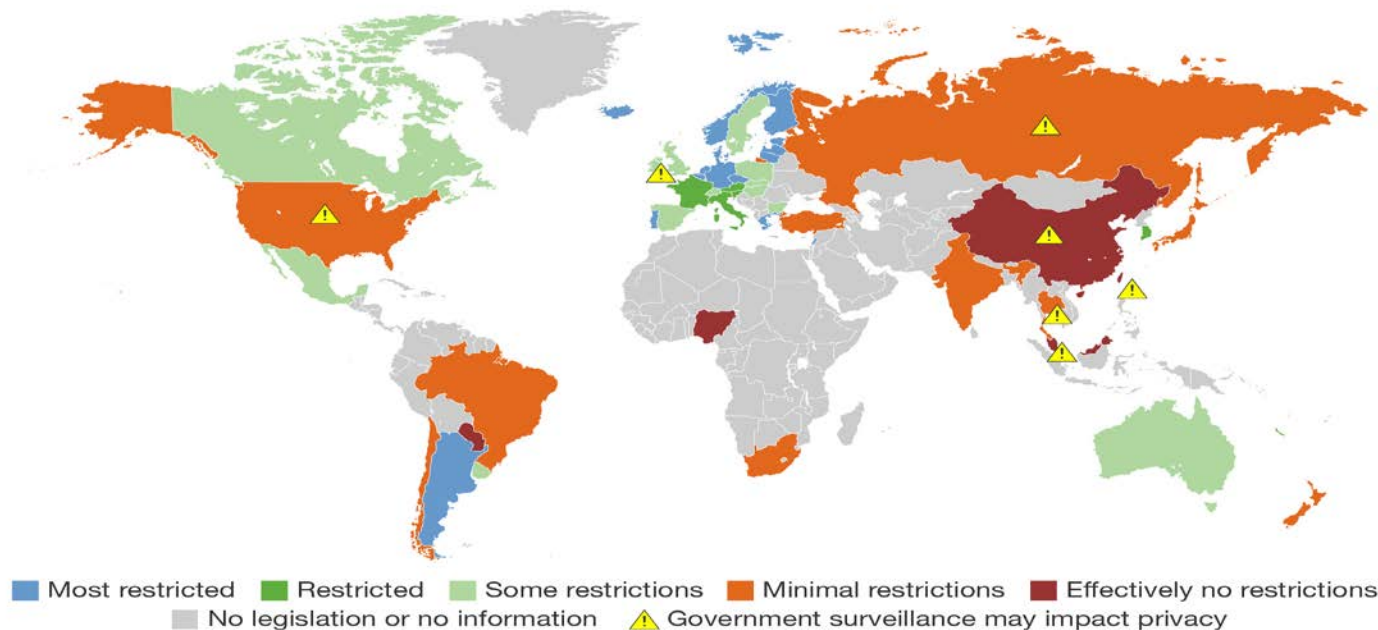
The background of the image shows several stacks of casino chips on a green felt surface. The chips are in various colors including black, yellow, purple, and orange. Some chips have numbers like '500' and '100' visible. The text is overlaid on the left side of the image.

Tokenization Supports Data Residency

Data Privacy is a global initiative



#RSAC



Source: US Department of Commerce and country-specific legislation

Source: August 2014 "Forrester's 2014 Data Privacy Heat Map" Forrester report



**Tokenization
Protects
Consumer
Privacy**



Privacy is a
value we all
care about

Privacy is a value we care about



#RSAC



46%

would **stop** shopping
from retailers who track
in-store behavior



27%

worry about
unintentionally granting
access to their info



22%

look for specific topics in
privacy policies



33%

have canceled a transaction
because of privacy concerns



Kill your data!



#RSAC

- Abstracting toxic data into a token mitigates the risks associated with data privacy and residency issues.
- Tokenization is a type of data loss prevention.
- Tokenized systems are typically not in scope (e.g. PCI)
- Tokenization can be applied to any Toxic Data string (00110100101001001000111101010)



Apply What You Have Learned Today



- Appoint a Data Champion
 - Do you have a Chief Data Officer?
 - Who is incentivized to Protect Data?
 - Treat Data as a Corporate Social Responsibility
- What Data should You Tokenize?
 - Classify Your Data based upon how you need to protect it.
 - Tokenization vs. Encryption
- Investigate Tokenization Technologies
 - Do you have a Data Encryption provider?
 - Rise of the API Economy
 - Focus of Management



Thank You



John Kindervag
+1 469.221.5372
jkindervag@forrester.com
@Kindervag

