The Legal Attack Vector: How To Protect Yourself

DANIEL P. COOPER
COVINGTON & BURLING LLP

CAROL UMHOEFER
DLA PIPER

- "In the Event of Breach…"

RSACONFERENCE
EUROPE 2012
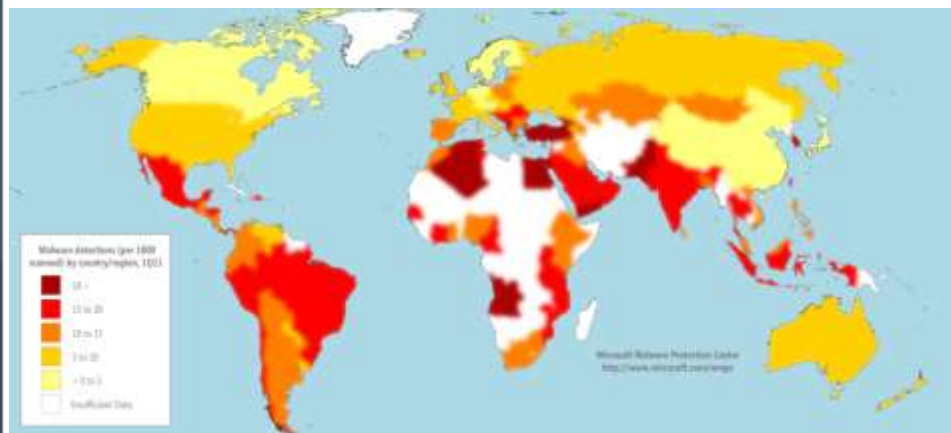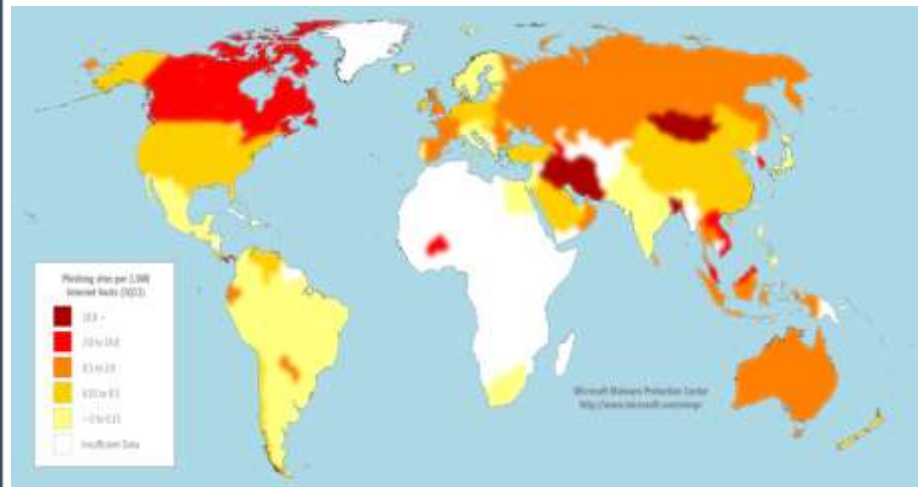
In the News - 1 October 2012

```
129.  Our targets for this release have been the top 100 universities around the world. After carefully filtering
      the ones that we've already leaked before and the ones where Anonymous has in major operations, we have
      eventually got together a new fresh list. The majority of them should be here. Also, some of us decided to go
      ahead and add vulnerable links to the other ones anyway, which you can find at the bottom, at "Other
      Universities".
130.
131.  side note* We tried to keep the leaked information to a minimum, so just around 120.000+ accounts and records
      are here, leaving in their servers hundreds of thousands more. (When we got there, we found out that a lot of
      them have malware injected. No surprise there since some have credit card information stored.)
132.
133.  Harvard - Mirror1: https://gist.github.com/3810660 Mirror2: https://privatepaste.com/92c03f31b3 Mirror3:
      http://pastesite.com/44824
134.
135.  Cambridge Server 1 - Mirror1: https://gist.github.com/3810676 Mirror2: https://privatepaste.com/e7c3e06a37
      Mirror3: http://pastesite.com/44825
136.
137.  Cambridge Server 2 - Mirror1: https://gist.github.com/3810701 Mirror2: https://privatepaste.com/d8b503fb6e
      Mirror3: http://pastesite.com/44828
138.
139.  Stanford Server 1 - Mirror1:
      https://raw.github.com/gist/3810691/5e96bca0192cfe34d8d9841d63f152ddbfbff6b4/gistfile1.txt Mirror2:
       https://privatepaste.com/82d024500e Mirror3: http://pastesite.com/44826
140.
```

The Threat Today

Malware Infection Rates by Country*

Malware Hosting Sites by Country*

Worldwide Phishing Sites*

The threat today is global and constant…!

COVINGTON & BURLING LLP

RSACONFERENCE EUROPE 2012

The Threat Todav

Figure 38. Threat category prevalence worldwide and in 10 individual locations, 2Q11

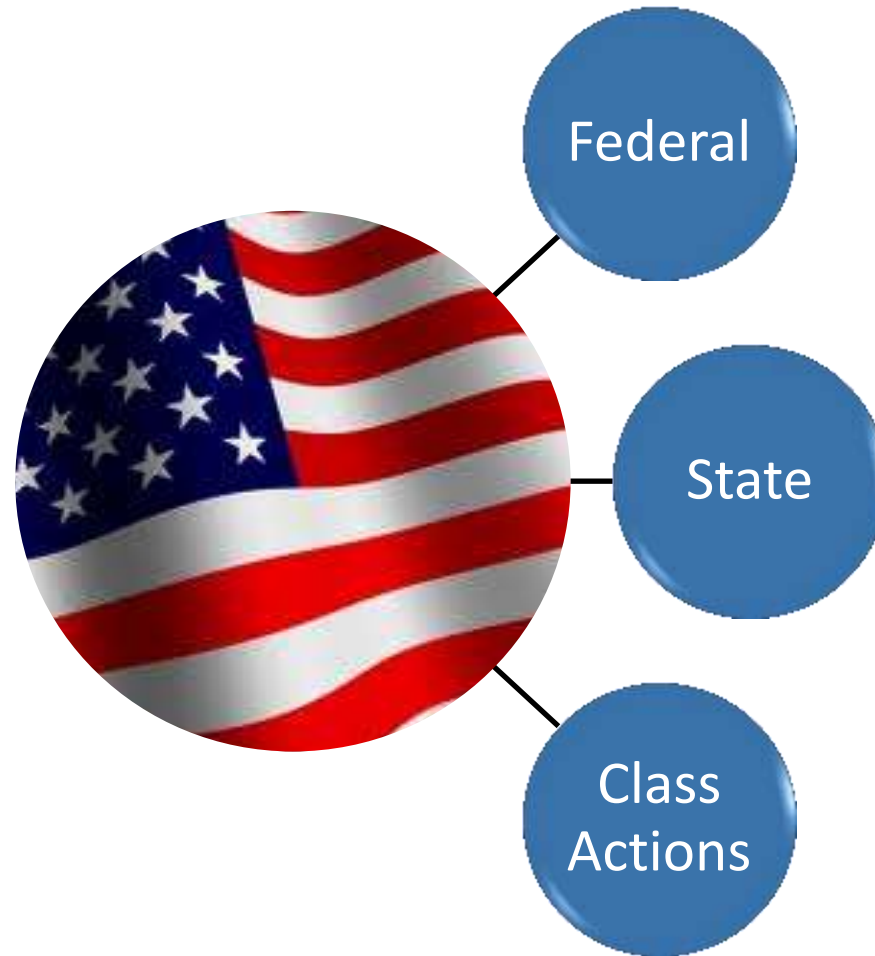| Category	World	US	Brazil	Fr.	UK	China	Ger.	Russ.	Italy	Can.	Tur.
Adware	37.0%	39.7%	26.1%	72.4%	49.1%	5.3%	44.1%	9.7%	60.0%	45.8%	37.7%
Misc. Potentially Unwanted Software	30.6%	22.1%	35.2%	27.7%	27.9%	48.8%	26.5%	60.3%	26.1%	26.7%	34.7%
Misc. Trojans	28.9%	38.9%	22.6%	12.1%	31.9%	36.6%	25.4%	34.1%	15.5%	36.2%	41.9%
Worms	17.2%	6.3%	24.2%	7.3%	5.9%	14.0%	8.6%	19.9%	11.9%	5.0%	31.3%
Trojan Downloaders & Droppers	14.7%	17.8%	21.0%	7.0%	13.8%	20.4%	13.4%	9.7%	9.1%	17.4%	13.5%
Exploits	10.0%	14.4%	16.3%	2.7%	10.5%	15.0%	7.9%	7.1%	4.0%	13.1%	3.4%
Viruses	6.7%	2.0%	10.1%	1.2%	3.4%	8.0%	2.9%	8.4%	1.7%	2.0%	17.7%
Password Stealers & Monitoring Tools	6.3%	2.9%	18.9%	2.4%	3.9%	4.8%	6.8%	5.1%	4.2%	2.8%	7.8%
Backdoors	5.8%	4.8%	7.7%	3.3%	3.9%	8.4%	5.8%	6.3%	7.1%	4.6%	5.4%
Spyware	0.3%	0.4%	0.1%	0.1%	0.2%	1.8%	0.2%	0.3%	0.1%	0.3%	0.1%

Totals for each location may exceed 100 percent because some computers reported threats from more than one category.
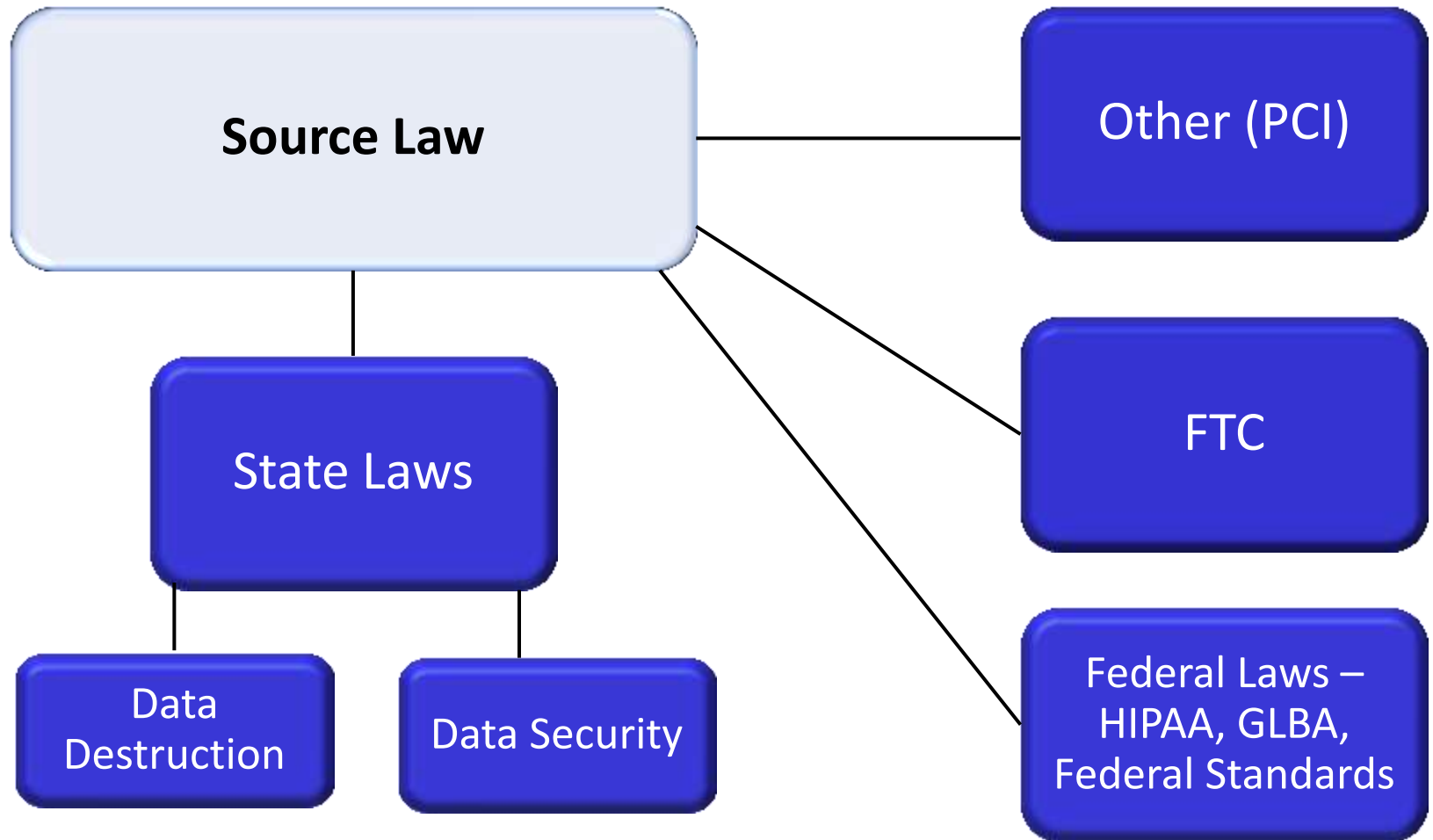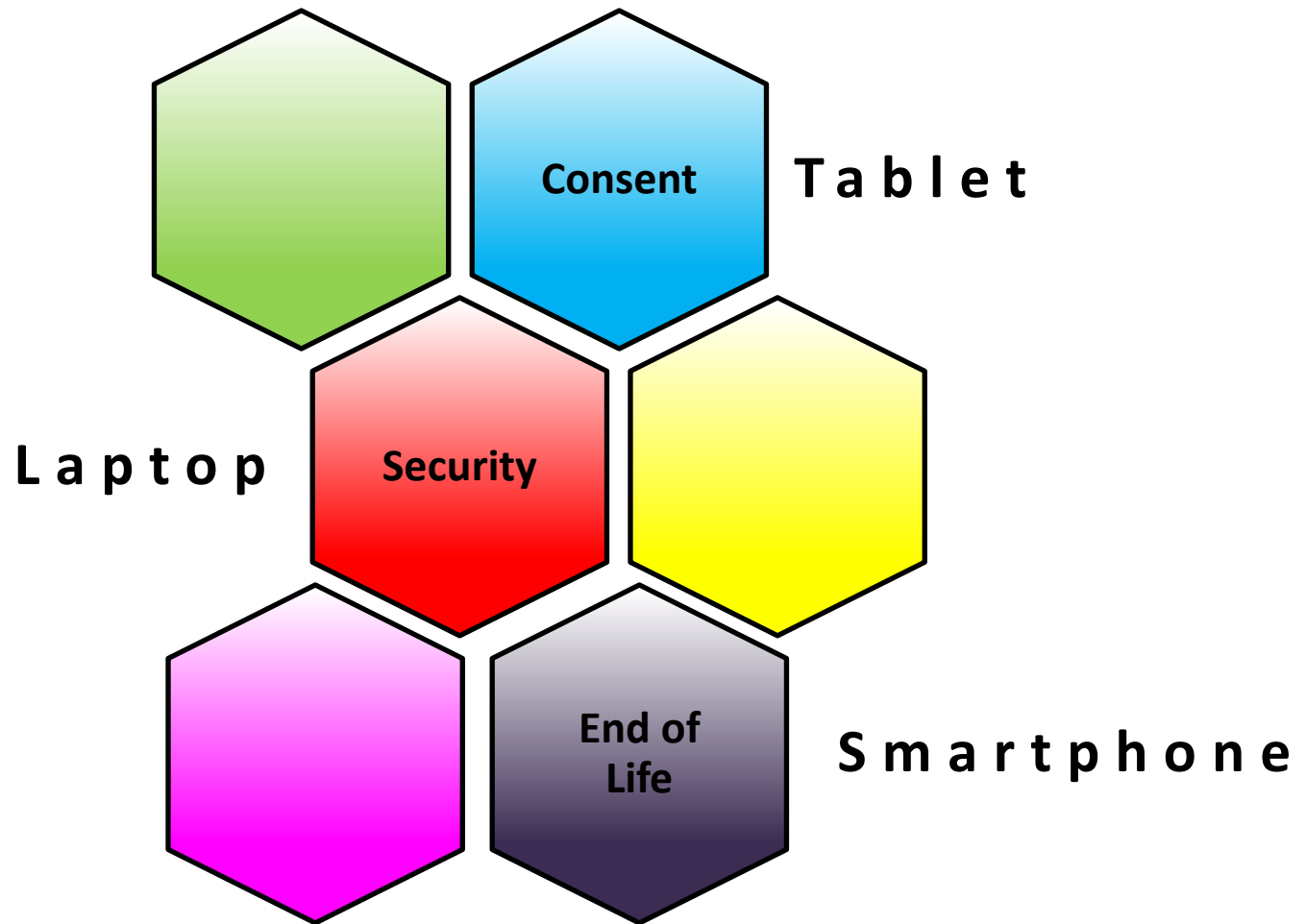
* Source: Microsoft Security Intelligence Report – Vol. 11

US Law

Federal

State

Class Actions

COVINGTON
COVINGTON & BURLING LLP

RSACONFERENCE
EUROPE 2012

Data Security

```
                    ┌─────────────────────┐                    ┌──────────────────┐
                    │                     │                    │                  │
                    │     Source Law      │────────────────────│   Other (PCI)    │
                    │                     │                    │                  │
                    └─────────────────────┘                    └──────────────────┘
                              │      \
                              │       \                        ┌──────────────────┐
                    ┌──────────────────┐\                      │                  │
                    │                  │ \                     │       FTC        │
                    │    State Laws    │  \                    │                  │
                    │                  │   \                   └──────────────────┘
                    └──────────────────┘    \
                        │          │          \                ┌──────────────────┐
          ┌──────────────┐   ┌──────────────┐  \               │  Federal Laws –  │
          │     Data     │   │     Data     │   \              │   HIPAA, GLBA,   │
          │  Destruction │   │   Security   │                  │ Federal Standards│
          └──────────────┘   └──────────────┘                  └──────────────────┘
```

Source Law

Other (PCI)

State Laws

FTC

Data Destruction

Data Security

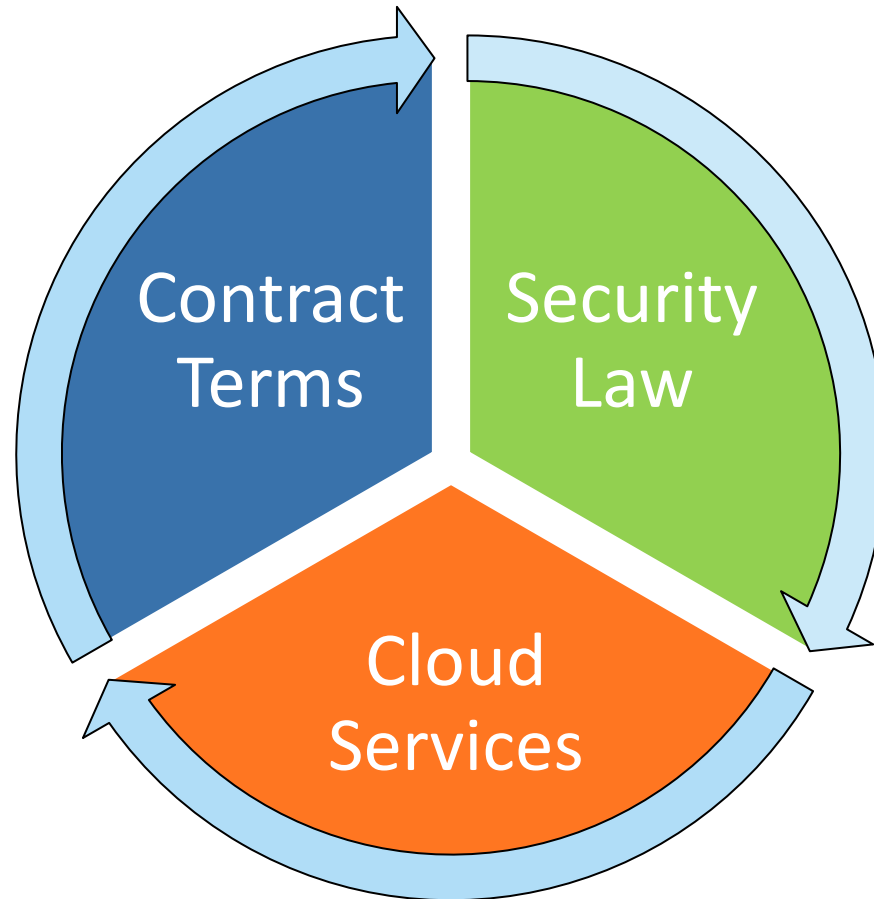Federal Laws – HIPAA, GLBA, Federal Standards

BYOD

Vendor Oversight

Data Breaches — Why It Matters

Litigation / Regulatory Risk

- <u>Consumers</u> or <u>shareholders</u>may sue

- Regulations in many states

- Breach of contract, common law torts
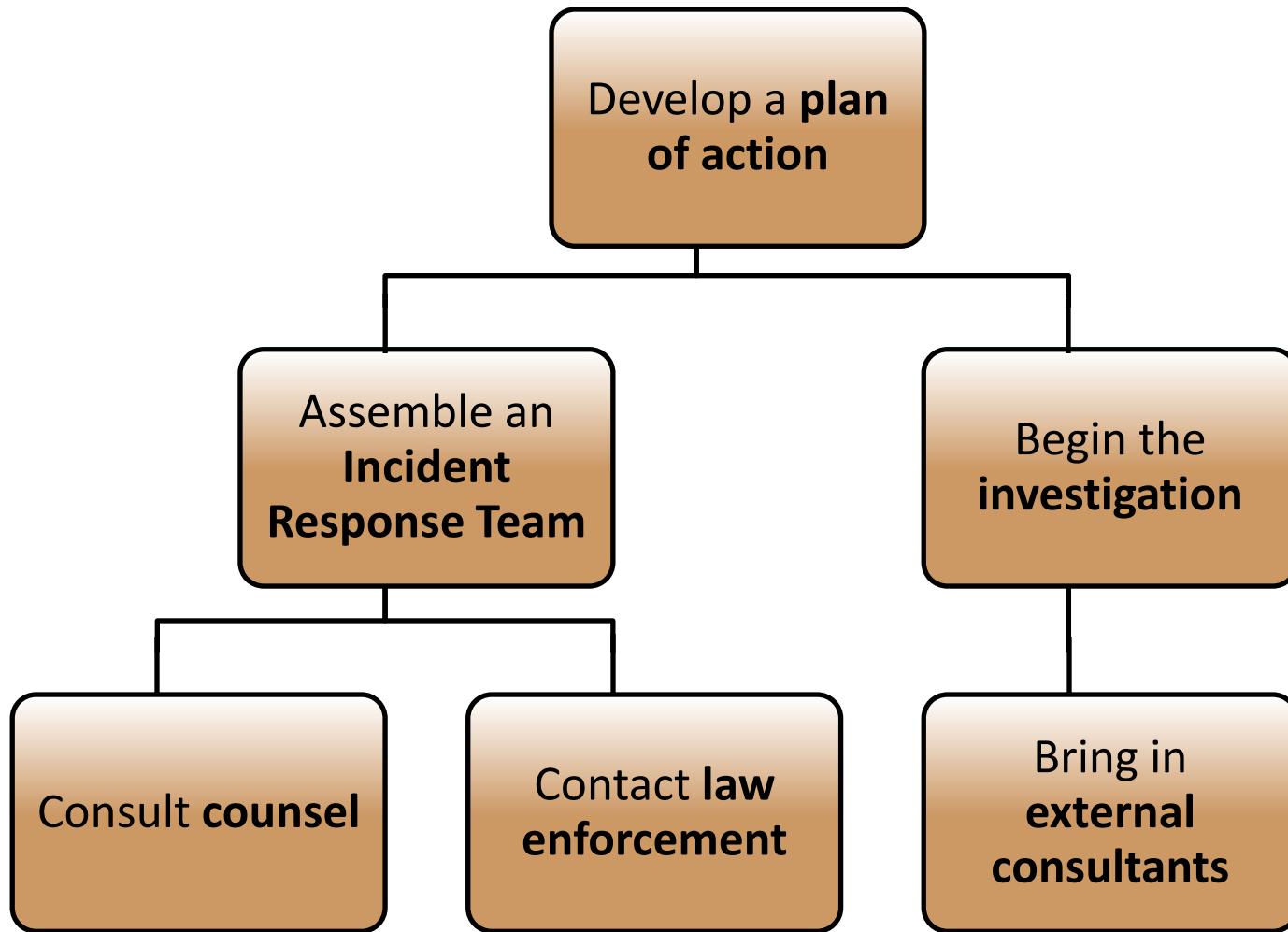
Contractual Risk

- Data security requirements in <u>service agreements</u>

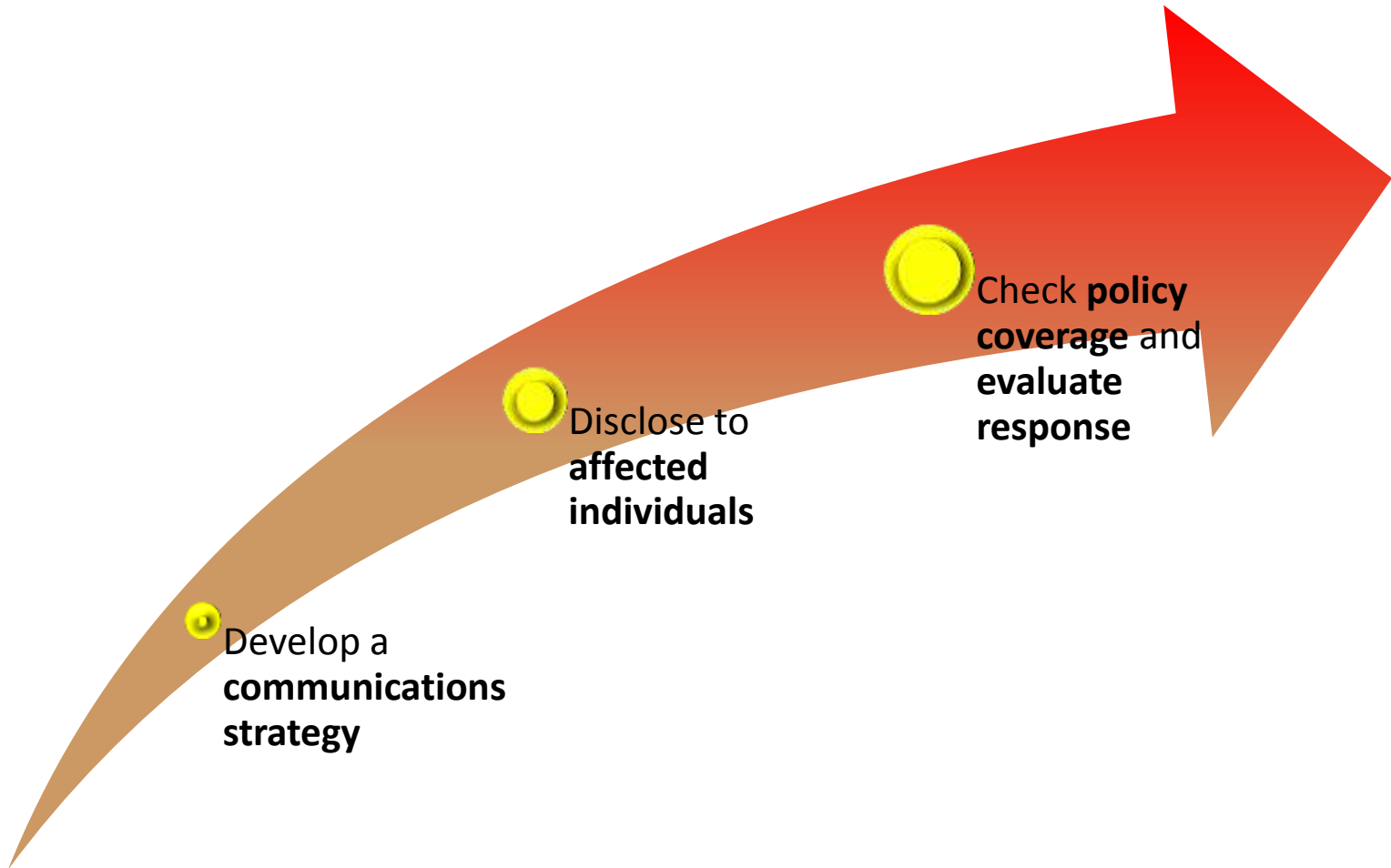- Obligations pursuant to PCI DSS (for credit card data)

Business/PR Risk

- Motivation for protection information also is <u>non-legal</u>

Key Considerations – First Steps

Key Considerations − Next Steps

Check **policy coverage** and **evaluate response**

Disclose to **affected individuals**

Develop a **communications strategy**

Checklist

Data Breach Key Considerations	
Plan of Action	❑
Incident Response Group	❑
Investigate	❑
Counsel	❑
Law Enforcement	❑
External Consultants	❑
Communication Strategy	❑
Disclosure	❑
Policy Coverage	❑
Evaluate Response	❑

Cross Border Transfers

- Less strict than EU
- Congressional activity
- Best practice

■ All You Need to Know About Transfers, Security, Breaches and BYOD:

A European Perspective

RSACONFERENCE
EUROPE 2012

Three Keys to Transfer Compliance

End-to-end encryption

Read-only is a transfer

Transfers ex-EU require TLC from lawyers

Carol A.F. Umhoefer
DLA Piper

RSACONFERENCE
EUROPE 2012

16

Three Keys to Understanding Security

Security is a poor cousin

"appropriate technical and organizational measures"

Different approach for each country

Carol A.F. Umhoefer
DLA Piper

RSACONFERENCE
EUROPE 2012

Three Rules on Breach Reporting

Providers of publicly available electronic communications services

ROW

Different approach for each country

Carol A.F. Umhoefer
DLA Piper

RSACONFERENCE
EUROPE 2012

Three Horrors of BYOD

Consent

Lawyers don't get what IT is doing (and vice versa)

The worst is yet to come

Carol A.F. Umhoefer
DLA Piper

Questions?

Daniel P. Cooper
Covington
dcooper@cov.com

Carol A.F. Umhoefer
DLA Piper
carol.umhoefer@dlapiper.com

RSACONFERENCE
EUROPE **2012**